PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS

DISERTACION PREVIA A LA OBTENCION DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

"APLICACIÓN DE LA NORMA ISO 27001 PARA LA IMPLEMENTACIÓN DE UN SGSI EN LA FISCALÍA GENERAL DEL ESTADO"

IVÁN RICARDO NARVÁEZ BARREIROS

DIRECTOR: ING. JAIME NARANJO

QUITO, 2013

DEDICATORIA

Dedico el presente trabajo a mi esfuerzo, por ser la recompensa justa al trabajo invertido. Lo dedico también a todos aquellas personas que aportaron, de cualquier forma, para que este camino concluya.

En particular a mi familia por estar presente en los altos y bajos, a los que tuvieron siempre el norte bien definido, ya que con su ejemplo yo pude definir el mío; y a todos aquellos que buscaron una forma para apoyarme.

En fin, está dedicado a la vida misma por darme la oportunidad de realizarlo y así poder descubrir otra cara más de Dios a través de la vivencia de las circunstancias, el esfuerzo en el trabajo, la recompensa en el conocimiento y la celebración en el reconocimiento.

Espero que este trabajo sea de apoyo a otros proyectos y que beneficie de manera positiva a muchas personas.

AGRADECIMIENTOS

Agradezco a todos aquellos que con su presencia hicieron un cambio trascendente en mi vida, a quienes con sus palabras o acciones pusieron ante mis ojos un camino de conciencia, donde el esfuerzo es recompensado, el camino es disfrutado y las metas celebradas.

Aquellos que sin saber con sus palabras abrieron mis ojos, a los que son su honestidad y firmeza normaron mi conducta, a aquellos que con su amor alivianaron la carga, a los que son su compañía alegraron mi vida.

Agradezco sobremanera a mi madre, a mi padre y mi hermana Daniela por estar ahí siempre, pese a la distancia o a las circunstancias. Los amo.

CONTENIDO

1. CAPÍTULO I – MARCO TEÓRICO

1.1 Conceptos y criterios de Seguridad de la información

En la actualidad, la información es el activo más valioso de cualquier compañía o institución. Sobre esta base se observa que, los gobiernos, entidades financieras, entidades de control, centros de salud, entidades gubernamentales, empresas privadas realizan esfuerzos para la automatización de sus procesos, a fin de obtener una mejor productividad y eficiencia, esto a su vez demanda y genera una gran cantidad de información, que puede ser confidencial (ya sea por el mandato de alguna normativa legal o por secretos de investigación o producción), abarcandodesde la información administrativa interna como datos personales de sus empleados, productos, situación financiera, etc, hasta información de facturación, rastreo de paquetes, datos de clientes, etc.

Centrándose en el área de gestión de la Fiscalía General del Estado, está institución mantiene una gran cantidad de información, mayormente en medios impresos, debido a las investigaciones que realizan los fiscales son sustentadas en documentos físicos, según la interpretación de normativa vigente, durante varias decenas de años. Así también cuenta con un conjunto igualmente grande de documentos de orden administrativo, siendo las direcciones de Recursos Humanos, Administrativo Financiero las que mayor cantidad de documentación archivan en las distintas zonas destinadas a este fin.

Esta información se recolecta desde varios puntos donde es receptada, procesada y almacenada para que se pueda utilizar por sus empleados y directivos con fines de trabajo (enriquecimiento de valor) y gerenciamiento (para la toma de decisiones) y esta puede ser transmitida por medios telemáticos dentro y fuera de las instalaciones de la empresa o institución.

Además, el valor de la información está en directa proporción por el uso que se pueda dar, sea esta por el generador o dueño de la información, que generalmente son los procesos relacionados con las Direcciones Administrativas, así como por el uso autorizado o no, de esta por otra persona o empresa. Han sido varios los casos que se

han denunciado acerca de organismos del sector público que han establecido políticas de seguridad inadecuadas en sus registros electrónicos posibilitando que terceros se apropien de la información custodiada y la puedan comercializar dentro y fuera del país con fines ilícitos.

De acuerdo a la temática del presente trabajo, es acertado el mencionar algunos conceptos que conforman la base para la implementación y que deben ser revisados y conocidos para que se puedan enunciar con propiedad, oportuna y de forma adecuada.

El planteamiento principal y objetivo de este documento es la aplicación de la ISO-27001 para la implementación de SGSI en la Fiscalía General del Estado, por tanto es necesario introducir algunos conceptos relacionados con estos términos, así como también la relación entre los distintos componentes que se mencionan.

De inicio, se observa una relación directa entre un SGSI y el concepto de información. A fin de poder establecer un lineamiento y contar con un universo de conceptos unificados, se agregarán algunas descripciones o definiciones, varias de ellas ya conocidas, pero a fin de obtener una integridad de conceptos se mencionarán de manera rápida.

Siendo el concepto de Información el eje central de donde parte la necesidad de la aplicación de una norma y un sistema de gestión en una institución pública o privada, se define como información a cualquier conjunto de datos que se encuentren organizados, que representan valor a la organización o institución a la que pertenecen, independientemente que estos se encuentren almacenados o transmitidos en forma escrita, gráfica, oral, en correo electrónico, en bases de datos, fax, formato de audio, etc. Ni tampoco de los orígenes que los mencionados datos provenga de fuentes externas o internas, ni de su fecha de elaboración o recepción.

Según Wikipedia, la información está definida como:“En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Para GillesDeleuze, la información es el sistema de control, en tanto que es la propagación de consignas que deberíamos de creer o hacer que creemos. En tal sentido

la información es un conjunto organizado de datos capaz de cambiar el estado de conocimiento en el sentido de las consignas trasmitidas.

Los datos sensoriales una vez percibidos y procesados constituyen una información que cambia el estado de conocimiento, eso permite a los individuos o sistemas que poseen dicho estado nuevo de conocimiento tomar decisiones pertinentes acordes a dicho conocimiento.

Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno."[1]

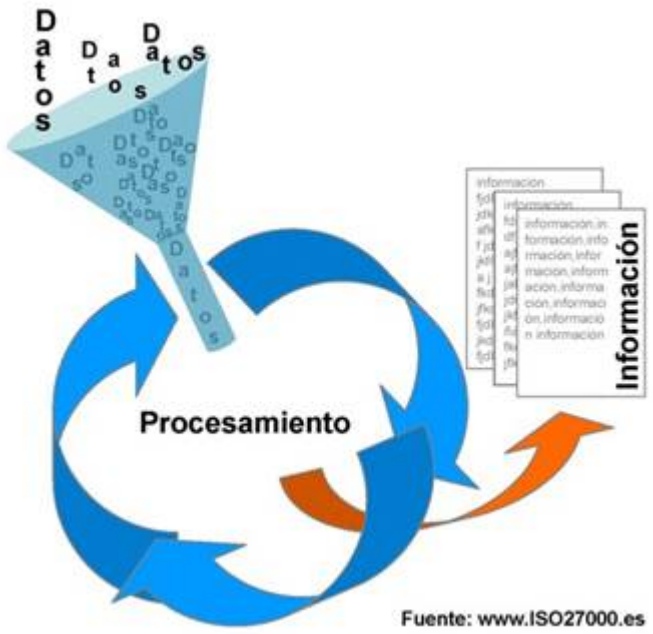


Diagrama Nro. 1 Esquematización de la transformación de Datos en Información[2]

Ejemplificando esta definición, puedo indicar que el un proceso inicial de contacto con el usuario externo, en la FGE realiza un conjunto de procesos de Atención al Público,

[1] Información – Información . Internet: http://es.wikipedia.org/wiki/Informaci%C3%B3n Acceso: 18/06/2012
[2] ISO27000.es – ¿Que es SGSI? . Internet: http://www.iso27000.es/sgsi.html#section2d Acceso: 25/03/2012

relacionados con Exámenes Médicos, Asesoría en la tipificación del Delito, Actividades Administrativas, entre otras, todas ellas se registran en el Sistema Informático, que procesa y almacena varias decenas de variables (en el caso más sensible, se registran alrededor de 50 variables en el documento de la Denuncia de Delito de Acción Pública) donde se combinan datos reservados y públicos, todos estos datos adquieren la categoría de información al momento de ser procesados de acuerdo a la necesidad que se quiera analizar y solventar. Por ejemplo, de un conjunto de denuncias ingresadas es posible obtener indicadores que sirven a varios procesos gobernantes o agregadores de valor. Un conjunto de indicadores que se utilizan diariamente en la gestión son derivados de los procesos representados en la cadena de valor de la institución, que se representa de la siguiente forma:

PROCESO GOBERNANTE

PROCESOS ESTRATEGICOS

PROCESOS AGREGADORES DE VALOR

Diagrama Nro. 2 – Cadena de Valor de la Fiscalía General del Estado[3]

Proceso Estratégico	Indicador	Aplicación del indicador

[3]Fiscalía General del Estado – Estatuto Orgánico por Procesos – Internet: http://www.fiscalia.gob.ec/images/LOTAIP/A/Estatuto_Orgnico_por_Procesos_FGE.pdf - 29 de Marzo de 2013

Gestión Estratégica	Número de proyectos para implementación de acuerdo al incremento o decremento de delitos en las provincias de la sierra	Mejorar, ampliar o agregar nueva infraestructura para mejorar el acceso de la ciudadanía a la investigación de los delitos
Gestión de Política Criminal	Cantidad de robo a personas desde las 00H00 hasta las 05H00 los días viernes	Coordinación con Policía Nacional o Policía Judicial para realizar operativos en los lugares y horas de alto índice delictivo
Gestión Procesal	Número de denuncias por Especialidad	Evaluación de carga laboral para reforzamiento mediante directrices o reestructuración de Especialidades
Gestión de Calidad	Número de ingresos equivocados por parte de los asesores	Mejoras en el procedimiento para evitar futuros errores

Tabla Nro. 1: Ejemplos de indicadores que pueden ser obtenidos desde una misma fuente de recolección de información, caso Denuncia de Acción Pública. Fuente: Elaborado por el autor

Como se observa, la misma fuente de recolección de datos, se puede convertir en el origen de información que será consumida por distintos actores y a distintos niveles de coordinación con otras instituciones, de ahí que si existiera un incidente que desemboque en la interrupción del flujo regular de información causaría una reacción en cadena que genera inestabilidad, pérdida de credibilidad e inseguridad en la ciudadanía, usuarios internos y directivos de la institución entre otros.

Para evitar este tipo de incidentes, se procede a presentar un proyecto de aplicación de la norma ISO 27000, para la creación de un Sistema de Gestión de Seguridad de la Información SGSI.

Un SGSI deacuerdo con la bibliografía consultada se definiría como:

"El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

…El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías."[4]

En otros términos, lo que busca un SGSI es asegurar de la manera más eficiente que la información disponga de confidencialidad, integridad y disponibilidad, considerando a la información como un activo importante en la empresa o institución, a la vez de gestionar los riesgos a la que esta pueda ser sometida.

[4] ISO27000.es – ¿Que es SGSI? . Internet: http://www.iso27000.es/sgsi.html#section2d Acceso: 25/03/2012

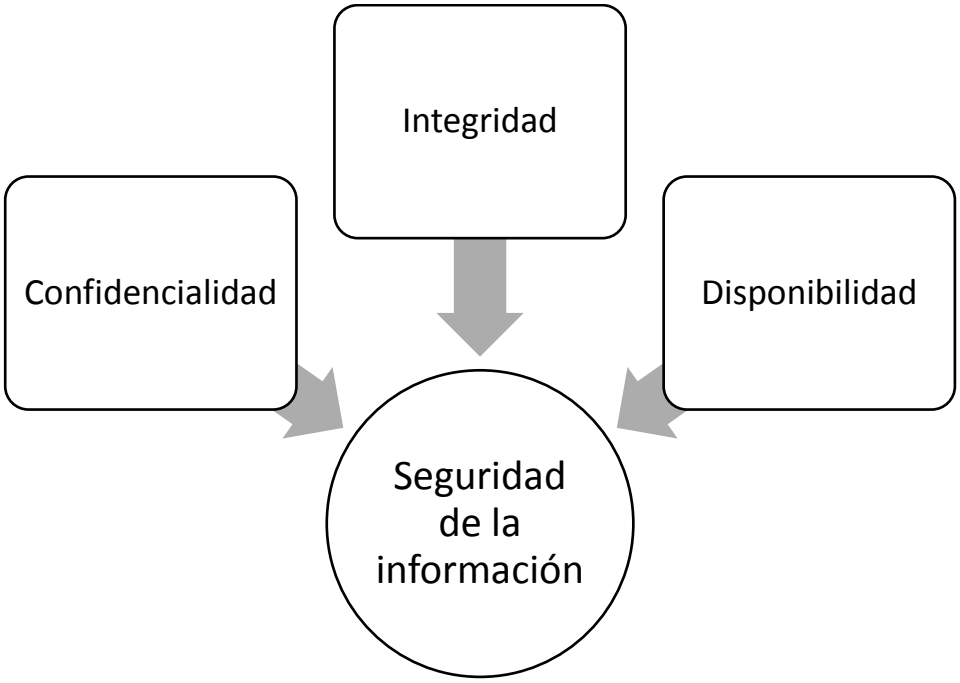


Diagrama Nro. 2 – Esquematización de los conceptos relacionados con la seguridad de la información. Fuente: Elaborado por el autor.

A fin de explicar algunos detalles concernientes a las particularidades de la institución en la que ser desea aplicar la norma, se expondrán los conceptos generales a los que se refiere la seguridad de la información.

En el caso de la Confidencialidad, es una propiedad de lainformación, por la que se pretende garantizar que dicha información se encuentre accesible únicamente por la o las personas que deben tener acceso. La confidencialidad ha sido definido por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 como "garantizar que la información es accesible sólo para aquellos autorizados a tener acceso" y es una de las piedras angulares de la seguridad de la información.[5]

En la FGE, gran parte de las investigaciones de los fiscales, ingresa a sus despachos como una etapa pre-procesal denominada “Indagación Previa”. Durante esta etapa todos las diligencias, resoluciones, solicitudes, oficios, nombres de los sospechosos, etc. Deben ser mantenidos en secreto por Ley, únicamente las partes involucradas

[5] Wikipedia – Confidencialidad – Internet: http://es.wikipedia.org/wiki/Confidencialidad - 31 de Marzo de 2013

directamente tienen acceso al expediente, donde figura toda la investigación del fiscal y su equipo de apoyo. Faltar a este principio generaría una nulidad en los procedimientos y podría quedar un crimen sin justo tratamiento, incrementando la conmoción social y desconfianza en el aparataje de la Justicia en el país, a esto se sumaría la cantidad de horas invertidas en la sustentación del caso por parte del Fiscal, agentes de la Policía, entidades financieras, otras instituciones del sector público, etc. Así mismo existen otras restricciones de carácter legal en delitos de Violencia Sexual e Intrafamiliar y los delitos cometidos por menores de edad, que incluso tienen una legislatura especial y son amparados por normas, leyes y convenios internacionales, lo que agudiza la necesidad de disponer de información que sean confidencial.

Refiriéndose a Integridad, en este tema, se refiere concretamente a la validez y consistencia de los elementos de información almacenados y procesados en los sistemas informáticos.

En este esquema, las distintas herramientas de seguridad informática deben garantizar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

En un sistema de alta concurrencia, el no disponer de procesos de Integridad de información coherentes, tendría un efecto caótico en la administración de información y en los resultados obtenidos. Por ejemplo, si existiera un problema con una denuncia relacionada con la duplicidad del mismo hecho, constaría una persona con dos procesos abiertos, que podrían estar con dos fiscales distintos, teniendo que invertir en dos abogados para defenderse de las acusaciones o impulsando la denuncia, así mismo existiría un dato inexacto en lo que corresponde a estadísticas delincuenciales, desembocando en políticas de seguridad pública equivocadas.

Finalmente, con Disponibilidad de la Información nos referimos a la posible continuidad de acceso a los elementos de información almacenados y procesados desde un sistema informático.

Las herramientas de Seguridad Informática deben reforzar la permanencia y disponibilidad delos sistemas informáticos, de tal forma que se presenten las

condiciones de actividad adecuadas para que los usuarios, tanto internos como externos, personal administrativo y directivo, puedan acceder a la información con la frecuencia y dedicación que requieran.

En este momento existen alrededor de 180 puntos de atención de la FGE a nivel nacional, distribuidos en 220 cantones y 24 provincias, además brinda soporte para procesos automatizados para alrededor de 1500 usuarios internos (500 fiscales y equipos de apoyo), información delincuencial detallada para 24 administradores de Policía Judicial, análisis estadístico interno, y público en general desde el portal www.gestiondefiscalias.gob.ec para consulta de denuncias, esto genera una gran cantidad de accesos concurrentes al sistema informático y nos indica que disponer de una infraestructura física y software de alta disponibilidad es un parte de un procedimiento crítico para esta institución.

Basándose en experiencias anteriores, el disponer de sitios alternos y respaldos de información no es el único recurso que se debe considerar al momento de pensar en Integridad de la información, sino disponer de documentación, planes de contingencia claros, procesos y roles bien definidos garantizan una mejor respuesta al momento de gestionar incidentes.

La interrupción del servicio en general, causa en muchos casos incomodidad a los usuarios externos, problemas con los usuarios internos, reclamos e inconvenientes que generan inseguridad y mala reputación de los sistemas que se generan, considerando que como un sistema, este está compuesto por distintas partes y si una de ellas falla todo el sistema perdería continuidad de servicio. Estos son casos muy comunes, donde los problemas de conectividad influyen mucho en el rendimiento general de todo el sistema.

En general, si no se dispone de Políticas y Normativa interna coherente, actualizada, socializada entre los usuarios del sistema, ajustadas dentro de un modelo de Gestión claro y conocido por todos los funcionarios, muchos de los esfuerzos para garantizar la seguridad informática no serían tan eficaces como podrían, así por ejemplo en un proceso de gestión enfocado en atención al público en general, para que sea válido, debe contar con un proceso de estabilidad a largo plazo (o con un esquema de transformación definido y calendarizado) disponiendo de la flexibilidad necesaria para

ajustarse a cambios internos como a las nuevas normativas que se pueden presentar en el futuro.

Hasta este momento, se ha expuesto algunos componentes o conceptos básicos relacionados con el tema que se expone, hemos revisado las diferencias entre dato e información, cuales son las propiedades de la información y algunos criterios de Seguridad Informática, con esta base podemos indicar con propiedad en que consiste un SGSI.

Actualmente en nuestro país, en lo que respecta al sector público, se muestra un creciente interés por el manejo sistemático y documentado de los procesos de cada organización, con una visión planificadora, con la finalidad de optimizar tiempo y recursos, a la vez, de justificar de mejor manera la inversión realizada por el estado. Así mismo se ha visto fuertemente impulsada los proyectos relacionados con la interconexión de todos los sistemas del Sector Público (a todos los niveles, como salud, educación, justicia, etc), Sector Bancario y otros sectores relacionados con el área productiva del país, a fin de poder disponer de un consolidado general de toda la información relacionada con los ciudadanos de este país.

Este proceso de integración o unificación del estado en el área de tecnología, evidencia la necesidad de poder constar con sistemas seguros, para que a su vez repliquen la información de forma correcta y oportunamente. Para garantizar dicha seguridad de la información esta debe ser gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

1.2 Métodos en el tema de seguridad de la información

Actualmente existen otros estándares, tanto ISO/IEC como No ISO, además de metodologías relacionadas con el tema seguridad de la información, manejo de riesgos y campos similares.

Se analizarán algunos estándares relacionados entre sí para observar algunas igualdades y diferencias entre ellos. Los estándares seleccionados son el ISO/IEC 13335, ISO/IEC 20000 y la norma AC SI 33 (norma no ISO, certificable).

ISO/IEC 13335

Esta norma ISO/IEC presenta los conceptos y modelos fundamentales para el entendimiento básico de Seguridades de las Tecnologías de Información y Comunicaciones y el manejo general de asuntos que son esenciales para un exitoso planeamiento, implementación y operación de ICT(Tecnologías de Información y Comunicaciones).

En este contexto, la intención de la norma no es sugerir un modo particular de enfoque de lo concerniente a la gestión de las tecnologías de información y comunicaciones, en lugar de esto, contiene un acopio de conceptos y modelos útiles para la administración de TICs. Es en general aplicable de muchas formas a diferentes ambientes de administración y organización. Esta organizado de tal manera que permite la adaptación dela norma para enfocarse en las necesidades de una organización específica y cualquier forma de administración.

Esta norma está organizada en dos partes:

Parte 1: Enfocada en conceptos y modelos para tecnología de información y comunicaciones, muestra una revisión de los conceptos fundamentales y modelos usados para describir la administración de seguridades de ICT (Tecnologías de Información y Comunicaciones)

Parte 2: Enfocado en Técnicas para manejo de riesgos de seguridad en tecnologías de información y comunicación. Describe además las Técnicas de Manejo apropiado de riesgos de seguridad para todos aquellos que se encuentran inmersos en actividades de administración.

Antes de las revisiones actuales, se presentan 5 partes que constituían 2 partes para descripción y manejo respectivamente además de reportes técnicos que corresponden a las partes 3, 4 y 5. En la versión en revisión, las anteriores partes 1 y 2 fueron reemplazadas por la parte 1 y las partes 3,4 y 5 serán reemplazadas por la parte 2, en las versiones revisadas.

ISO/IEC 20000

Esta norma está diseñada para proporcionar mejores servicios de TI, para clientes de una determinada organización, enfocado en su mayor parte para empresas proveedoras de servicios de TI.

Esta norma surge de la norma BD15000 que estaba relacionada con ITIL, cuenta con 13 procesos definidos, un proceso para planificación e implementaciones de los servicios de TI, enumera los requerimientos para un sistema de gestión y como otros estándares está enfocada en la mejora continua mediante el ciclo PDCA.

Uno de los propósitos principales de esta norma es conseguir una mejor orientación de los servicios hacia los deseos del cliente o usuario, además de integrar los distintos procesos de una organización para evitar que existan descoordinaciones o procesos asilados, todo esto a la par de mejorar los servicios ofrecidos en concordancia con la cadena de valor organizacional, dentro del esquema de mejora continua en todos los procesos.

Se encuentra relacionado con la gestión de manejo del ISO 9001:2000 basados en los principios de BPM, además de alinearse con los procesos organizacionales de tecnologías de la información, que entran dentro del ámbito de manejo de ITIL.

Esta ISO no ofrece lineamientos específicos de como diseñar los procesos, es más bien un conjunto de requerimientos que deben ser obligatoriamente cumplidos para poder acceder a una certificación. En este punto es donde ITIL ingresa como una parte importante, en particular la versión 3, debido a que se encuentra fuertemente alineado con esta norma, agregando una detallada colección de buenas prácticas, que es la base para iniciar el diseño de la ISO 20000. Iniciar el proceso de aplicación de la norma con la introducción de ITIL en los proceso de TI, facilita el cumplimiento de los requerimientos mínimos para la certificación en esta norma.

Según la bibliografía consultada, se necesita entre 12 y 24 meses para la iniciar el proceso de certificación en esta norma, plazo variable debido al grado de madurez de los procesos organizacionales.

ACSI33

Es una norma presentada por las oficinas del gobierno Australiano, refiriéndose a esta como una Manual para la seguridad de las Tecnologías de la Información y las comunicaciones.

Esta norma detalla los estándares mínimos de protección de los recursos de este gobierno, incluyendo la información personal y bienes; todas las agencias deben cumplir con esta normativa en sus operaciones.

Cada requerimiento de este estándar está supeditado en un sub-requerimiento más específico y este puede ser localizado en los principios de Seguridad que los motivan y los Patrones de diseño que satisfacen alguna necesidad en particular.

Está divido en 3 partes:

Parte 1: Corresponde a la norma y descripción de la seguridad en las TICs.

Parte 2: Define los roles y responsabilidades, manejo de riesgo de seguridad, políticas de seguridad, documentación de seguridad, planes de sistemas de seguridad, procedimientos de operaciones estándar, metodología de acreditación, mantenimiento y manejo de incidentes.

Parte 3: Lo referente a los estándares mencionados: seguridad física, seguridad de personal, ciclo de vida de los productos de TICs, seguridad de Hardware y Software, control de acceso lógico, seguridad activa, seguridad de comunicaciones y red, transferencia de datos.

Una particularidad de este estándar, es que cuenta con secciones que son segregadas entre Clasificadas y Desclasificadas, variando desde acceso público hasta acceso restringido dentro de ciertos perfiles a cierto tipo de controles.

Estanorma se encuentra en concordancia con ISO/IEC 17799:2006 – *Information technology – Code of practice for information security management*, y ISO/IEC 27001:2006 – *Information technology – Security techniques – Information security management systems – Requirements.*

		ISO		NO ISO
Norma	**ISO/IEC 27001**	**ISO/IEC 13335**	**ISO/IEC 20000**	**ACSI33**
Descripción Original	Tecnologías de la Información – Técnicas de Seguridad – Administración de Técnicas de Seguridad para la Información - Requerimientos	Administración de Seguridad de Tecnologías de la Información	Administración de Servicios de Tecnologías de la Información	Manual de Seguridad para Tecnologías de la Información y comunicaciones del Gobierno Australiano
Certificable	SI	NO	SI	SI
Ámbito o campo de acción	Engloba todas las áreas donde se puedan presentar incidentes en cuanto a seguridad de la información	Modelo de gobernabilidad de seguridad de la información amparado por la gobernabilidad de Tecnología de la Información o enfocado totalmente a los aspectos de tecnología de la información	Mayormente enfocado a organizaciones donde los servicios de tecnología son imprescindibles o fuertemente relacionados con el giro del negocio. Ej. Salud, entidades financieras, entidades públicas, etc.	Área de Tecnologías de la información, con obligatoriedad dentro del gobierno australiano
Ámbito de Recursos Humanos	Se definen responsables para las distintas áreas relacionadas con el manejo o consumo de la información para evitar o gestionar incidentes en seguridad de la información	Experto en seguridad debe conocer varios campos como comunicaciones, base de datos, etc.	Se definen responsables para las distintas áreas relacionadas con el manejo o consumo de la información	Define responsabilidades mediante SOP (Security Standard OperatingProcedures) a nivel de instrucciones a distintos niveles de uso o consumo de la información.

Gestión con Terceras Partes	Riesgos asociados al intercambio de la información	A través de salvaguardas, algunas de ellas obsoletas tras la publicación de ISO/IEC 27005:2008 y la norma ISO/IEC 18028-1:2006	Terceras partes o proveedores son integrados en la cadena de servicios	Terceras partes y proveedores son involucrados como parte de proyectos, conjuntamente con propietarios, usuarios.
Continuidad del servicio	Marco de gestión de continuidad, se incluyen los planes de contingencia	Evaluación general de los riesgos y vulnerabilidades de los sistemas, servicios y procesos de TI	A nivel de Planes de contingencia	Enfocado a las áreas de Infraestructura y Comunicaciones, mediante un SSP (System Security Plan)
Análisis de Riesgos	Identificación de riesgos asociados a la seguridad de la información de forma genérica.	Identificación, análisis y evaluación de riesgos de forma detalladas en varios capítulos, con explicación y ejemplos.	Riesgos asociados a la prestación de servicios de TI	Define y estructura un plan de gestión de riesgos para servicios de TI en entidades Gubernamentales australianas, estableciendo el contexto, diagnóstico, causas y consecuencias de los riegos
Gestión de Incidentes	Metodología para gestión de incidentes	El objetivo principal de la norma es ofrecer lineamientos, no soluciones, para gestionar incidentes de seguridad y presentar las salvaguardas apropiadas para cada caso.	Metodología para gestión de incidentes	Define responsabilidades mediante SOP (Security Standard OperatingProcedures) a nivel de planes de reconocimiento, auditoría de incidentes y responsables de procesos

Planificación de la capacidad	Define controles específicos que exigen que se garantice el rendimiento futuro de los sistemas a través de monitorizaciones a fin de predecir nuevas necesidades	A través de salvaguardas se prevé gestionar los riesgos, sin embargo definiciones específicas para la gestión de la capacidad solo se observan desde la perspectiva de evaluación de la vulnerabilidad que puede provocar.	Procesos explicados detallada y complemente con la finalidad primaria de garantizar la capacidad necesaria para proporcionar los servicios	Estructura proyectos que involucra a varios componentes interesados en ciertos servicios como por ejemplo los propietarios, usuarios, incluidos los proveedores o terceros.

Tabla Nro. 2: Cuadro comparativo de distintas normas ISO/IEC y no ISO en temas relacionados con seguridad de la información. Fuente: Varios autores.

Análisis de la comparación de los estándares ISO/IEC 13335, ISO/IEC 20000, AC SI 33 y la norma ISO/IEC 270001

Una vez realizados los cuadros comparativos desde donde se observan las similitudes y diferencias entre distintas formas de abordar el tema de seguridad de la información, se procede a hacer un análisis de los resultados obtenidos para verificar la idoneidad de la norma ISO/IEC 270001 para los temas de seguridad de información.

Uno de los objetivos que impulsan este proyecto es el poder obtener una certificación oficial para estos procedimientos, ubicando a las normas ISO/IEC 270001, ISO/IEC 20000 y AC SI 33 como las opciones ideales que podrían satisfacer este requerimiento.

Otro punto importante es la posibilidad de poder abarcar todas las formas posibles de información que se pueden presentar en la FGE. Como se indicaba en los anteriores puntos de este tema, la información presente se encuentra dispersa y en distintas formas, tanto a nivel nacional, en los distintos puntos de atención como en otras instituciones que conforman parte del diario accionar de la institución; así también en medios impresos y digitales incluyendo información multimedia que luego es presentada ante los jueces u otros actores que participan en la investigación del delito. En este aspecto, la norma ISO/IEC 27001 es aquella que puede participar en este contexto, debido principalmente a que el resto de normas se centran en la seguridad de las comunicaciones, servicios e información que maneja Tecnologías de la Información, dejando de lado otros temas relacionados con procedimientos o procesos fuera del área de tecnología.

Así mismo, en la normaISO/IEC 27001, se consideran de manera más efectiva la gestión del talento humano, debido a que en su aplicación se definen roles y responsabilidades en todos los procesos relacionados con custodia, procesamiento y consumo de información, en contraposición con la norma ISO/IEC 13335 donde se observa que el experto de seguridad debe disponer de conocimientos en varias áreas de TI, relacionadas con las comunicaciones, bases de datos, etc; agregando un posible componente de fallo en estos temas. Por otro lado las normas ISO/IEC 20000 y AC SI 33 si definen los roles y responsables de cada área de distinta forma, en el segundo caso a través de procedimientos de seguridad, que cuentan con cláusulas confidenciales que agregan cierto nivel de seguridad adicional.

Debido al rápido crecimiento de los servicios, planes administrativos y modelos de gestión distintos y autoridades de turno, el área de tecnologías de la información ha sido considerada una dependencia administrativa de segundo orden, básicamente porque siempre se limitó a ofrecer servicios básicos, poco especializados y enfocados a satisfacer necesidades de oficina y comunicaciones en un esquema limitado. Con una visión un tanto distinta, se ha propulsado procedimientos más elaborados con la finalidad de mejorar el desempeño en el área de trabajo de los fiscales, además también de los servicios de atención al público en general, servicios de comunicación interinstitucional, índices delictivos estadísticos unificados, catálogo de delitos, etc. Todos estos nuevos requerimientos han determinado en algunas áreas la necesidad de trabajar de forma más cercana con proveedores de servicios y equipamiento para usuarios finales como a procesamiento de información. Con este antecedente el disponer de esquemas de trabajo con terceros (en la calidad que sea) es una parte importante de los objetivos de mejoramiento que se desea alcanzar enfocadas fuertemente hacia dos perspectivas, la primera el intercambio de información entre los distintos actores del sector justicia y una segunda relativa a los servicios que TI ofrece tanto a usuarios internos, externos y otras instituciones. En el primer caso la ISO/IEC 27001 ofrece un conjunto de lineamientos enfocados estrictamente al intercambio de información, mientras que la ISO/IEC 20000 al estar enfocada en el área de los servicios de TI ofrece la alternativa óptima, debido a que agrega a la cadena de servicios, como se explica en la Tabla Nro.2, las otras normativas observan estos mismos conceptos, pero a través de lineamientos más descriptivos sin involucrarse en aspectos singulares de esta área.

Los distintos sistemas informáticos se encuentran enfocados mayoritariamente en esquemas de integración y unificación de procesos a nivel nacional, muchos de estos han sido discrecionalmente utilizados debido a servicios itinerantes como acceso a servicios de red, acceso a información de bases de datos, acceso a internet y correo electrónico entre otros. Esto abrió la posibilidad que dentro de un esquema de trabajo planteado, aprobado, implementado y socializado, se estén utilizando procedimientos alternativos en algunos procesos debido a que no tienen acceso a las herramientas informáticas o a las comunicaciones enviadas, claro es el ejemplo de que en algunos

lugares, el servicio de red o internet funciona con deficiencia lo que obliga a los funcionarios a receptar las denuncias en procesadores de texto en lugar del sistema informático misional acarreando posteriormente problemas en la evaluación de los fiscales, problemas en el seguimiento de la causa, posibilidad a posibles problemas de corrupción y confidencialidad de la información sensible de las denuncias y expedientes. Estos entre otros son los planteamientos que obligan a disponer de sistemas de alta disponibilidad o contar con un plan de continuidad del servicio elaborado, aplicable y en uso en la institución

Las normas de la serie ISO/IEC 27000 ofrecen un conjunto de normas relacionadas entre sí para el entendimiento, implementación y operatividad de un SGSI, sin embargo la ISO/IEC 27005 es la sección encargada de analizar de forma exhaustiva los riesgos desde la perspectiva o contexto de seguridad de la información, en esta norma se observa de manera clara la evaluación y tratamiento de riesgos. Por otra parte la norma ISO/IEC 13335 es la norma especializada para el análisis de riesgos, la ISO/IEC 20000 observa este ámbito desde los servicios de TI y AC SI 33 los observa dentro de la misma área con cierto nivel de exhaustividad en gran parte debido a que esta se encuentra alineada con la norma ISO/IEC 27001 y como soporte básico para las agencias gubernamentales. En el contexto de seguridad de la información, es imperante el poder contar con una análisis y evaluación de riesgos adecuado, por cuanto este es un requisito dentro de cualquier esquema de gestión que busque proteger la información. El grado de detalle y afinidad entre otros conceptos son los que definen que método o normativa utilizar, no obstante la normativa ISO/IEC 27001 observa estos procedimientos de manera generalizada como parte de implementación.

En un proyecto de automatización y tecnificación de los procesos, estos se ven inmersos en interacciones de conjuntos más grandes componentes, donde un mal funcionamiento de uno solo de estos pueda ocasionar problemas de toda índole, sin mencionar que en una institución donde el valor agregado son componentes jurídicos o legales y donde cualquier procedimiento mal encaminado puede causar la nulidad de procesos donde se ha invertido muchos recursos y tiempo es imperante el poder contar con lineamientos ordenados y estructurados para manejar los posibles incidentes que se pueden presentar. En este caso las normativas ISO/IEC 27001 y ISO/IEC 20000 ofrecen lineamientos muy claros para ofrecer los procedimientos adecuados para la

gestión de incidente, adicionalmente se puede mencionar que la ISO/IEC 20000 al estar alineado fuertemente con ITIL, ofrece una mayor cobertura desde el punto de vista de operatividad, sin embargo al ser un proyecto de implementación inicial, el agrupar y organizar los procedimientos se observa mejor desde una inspección general de la normativa a la que se desea certificar para luego alinear los procesos y servicios a ITIL y sobre esta base el proponer una certificación múltiple cuando sea factible hacerlo en los procesos que sean factibles.

La gestión de incidentes está cubierta como un modelo completo de gestión tanto en la ISO/IEC 27001 como en la ISO/IEC 20000.

Definir controles que puedan gestionar la capacidad de ofrecer un servicio es un punto que se encuentra implícito en cualquier unidad de tecnología, para este caso las normas ISO/IEC 27001 y ISO/IEC 20000 ofrecen las mejores alternativas para gestionar este aspecto.

De las explicaciones anteriores, en resumen se puede presentar este cuadro, mediante una escala de validación, en donde:

Valor	Significado	Descripción
1	Peor opción	No cumple con todos los requerimientos establecidos
2	Opción Intermedia	Cumple de manera básica los requerimientos solicitados
3	Mejor opción	Cumple de manera óptima los requerimientos establecidos

Tabla Nro. 3: Tabla de valoraciones para determinar la idoneidad de una norma frente a otras en el tema de seguridad de la información. Fuente: Elaborado por el autor.

		ISO		NO ISO
Norma	**ISO/IEC 27001**	**ISO/IEC 13335**	**ISO/IEC 20000**	**ACSI33**
Certificable	3	1	3	1
Ámbito o campo de acción	3	2	2	1
Ámbito de Recursos Humanos	3	2	3	2
Gestión con Terceras Partes	3	2	2	1
Continuidad del servicio	3	1	2	2
Análisis de Riesgos	2	3	2	2
Gestión de Incidentes	3	1	3	2
Planificación de la capacidad	2	1	3	2
TOTAL	22	13	20	13

Tabla Nro. 4: Tabla de resultados de las valoraciones en función de los criterios establecidos. Fuente: Elaborado por el autor.

De este análisis se puede concluir que la Norma ISO/IEC 27001 ofrece mejores prestaciones para los parámetros de evaluación.

1.3 Análisis de la situación actual de la Fiscalía General del Estado - Giro del negocio

La Fiscalía General del Estado es una institución que pertenece al sector Público, concretamente forma parte de la Función Judicial de nuestro país, no obstante tiene independencia tanto administrativa como financiera, según se desprende de las secciones y artículos de la Constitución Vigente: “

Sección décima

Fiscalía General del Estado

Art. 194.- *La Fiscalía General del Estado es un órgano autónomo de laFunción Judicial, único e indivisible, funcionará de forma desconcentrada y tendrá autonomía administrativa, económica y financiera. La Fiscal o el Fiscal General es su máxima autoridad y representante legal y actuará con sujeción a los principios constitucionales, derechos y garantías del debido proceso.*”[6]

La función principal de la FGE es la investigación de ciertos delitos, estos delitos son catalogados como delitos de “Acción Pública”. Esta clasificación es determinada principalmente por estar tipificados en el Código Penal del Ecuador (y son atendidos mediante el Código de Procedimiento Penal). Adicionalmente, se puede indicar que también existen otros tipos de delitos pero que son competencia de investigación de otras instituciones como Juzgados de Contravenciones, Comisarías, Intendencias, etc

La disposición para la realización de estas funciones de investigación esta también mencionada en la Constitución del Ecuador:

[6] Asamblea Nacional Constituyente - Constitución del Ecuador – Internet: http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf - 29 de Marzo de 2013

"***Art. 195***.- *La Fiscalía dirigirá, de oficio o a petición de parte, lainvestigación preprocesal y procesal penal; durante el proceso ejercerá laacción pública con sujeción a los principios de oportunidad y mínimaintervención penal, con especial atención al interés público y a losderechos de las víctimas. De hallar mérito acusará a los presuntosinfractores ante el juez competente, e impulsará la acusación en lasustanciación del juicio penal.*

Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistemaespecializado integral de investigación, de medicina legal y ciencias forenses,que incluirá un personal de investigación civil y policial; dirigirá el sistemade protección y asistencia a víctimas, testigos y participantes en el procesopenal; y, cumplirá con las demás atribuciones establecidas en la ley."[7]

De este último artículo, se puede ya visionar el alcance y magnitud de la responsabilidad de estas funciones de esta institución y por consiguiente también de la información que es recolectada y que debe ser presentada ante el representante de la Defensoría Pública y/o defensa de la parte acusada y los jueces, para sustentar un dictamen acusatorio, abstentivo o mixto una o varias personas.

Esta información constituye un área de vital importancia, por tanto debe estar organizada, disponible y custodiada con el mayor rigor, debido principalmente por las implicaciones que podrían repercutir a todos los participantes del proceso penal: fiscal, defensor, juez y acusado, además de otras instituciones relacionados con el sistema penitenciario y de Derechos Humanos.

Basados en la premisa referente a la responsabilidad de dirigir la investigación Preprocesal y procesal penal, se recaba gran cantidad de información que abarca desde testimonios de los involucrados, información bancaria, antecedentes policiales, diagramas de investigación, reportes policiales, exámenes médicos, solicitudes y reportes de audiencias, diligencias a otras instituciones, procedimientos documentales internos como externos, todos estos como parte delos procedimientos propios de la investigación que se menciona.

[7] Asamblea Nacional Constituyente - Constitución del Ecuador – Internet: http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf - 29 de Marzo de 2013

Sin embargo, existen otros procedimientos que se encuentran también relacionados con las actividades de los fiscales, pero que se engloban y enfocan desde otra perspectiva, como es el análisis cualitativo de las actividades por el fiscal solicitadas, control jurídico, estadísticas delincuenciales, sistemas de georeferenciación de delito, análisis de carga laboral, recursos humanos y administrativos, que también forman parte del patrimonio de información de la institución.

Toda esta información, se encuentra registrada en distintos formatos y en distintos lugares, hasta el año 2010, la mayor parte de la información se encontraba concentrada en los Archivos Centrales de cada provincia, básicamente en formato escrito y sin un mayor control en cuanto a la ubicación y remitente de los expedientes.

A partir del año 2010 se encuentra sistematizado un conjunto de procesos enfocados mayoritariamente en la Atención a la Víctima, además de un Nuevo Modelo de Gestión donde se utiliza como principal herramienta un sistema informático desarrollado in-house denominado SIAF.

Este sistema informático maneja un conjunto grande de variables mayoritariamente almacenadas en una Base de Datos y en documentos digitalizados, desde donde se pueden sacar estadísticas de gestión de los empleados, así como también un conjunto de indicadores de interés nacional, mayoritariamente enfocados a Seguridad Ciudadana.

La mayor parte de la información, este momento, es ingresada desde el proceso denominado Servicio de Atención Integral, enfocado mayoritariamente en la Atención de la Víctima (especialmente en campos como delitos de Lesiones y de Violencia Sexual), registro de actividades de un Asesor Fiscal, registro de denuncias, entre otras actividades administrativas.

Estas actividades a la par son también realizadas por agentes de la Policía Judicial y pronto se extenderá a otras instituciones también.

Se este proceso se obtienen alrededor de 200 variables que son posteriormente analizadas para el manejo de estadísticas tanto delincuenciales como de administración gerencial.

Sin embargo existen una gran variedad de sistemas tanto automatizados como domésticos de cada unidad que registran información valiosa, que complementa la gestión integral de la institución.

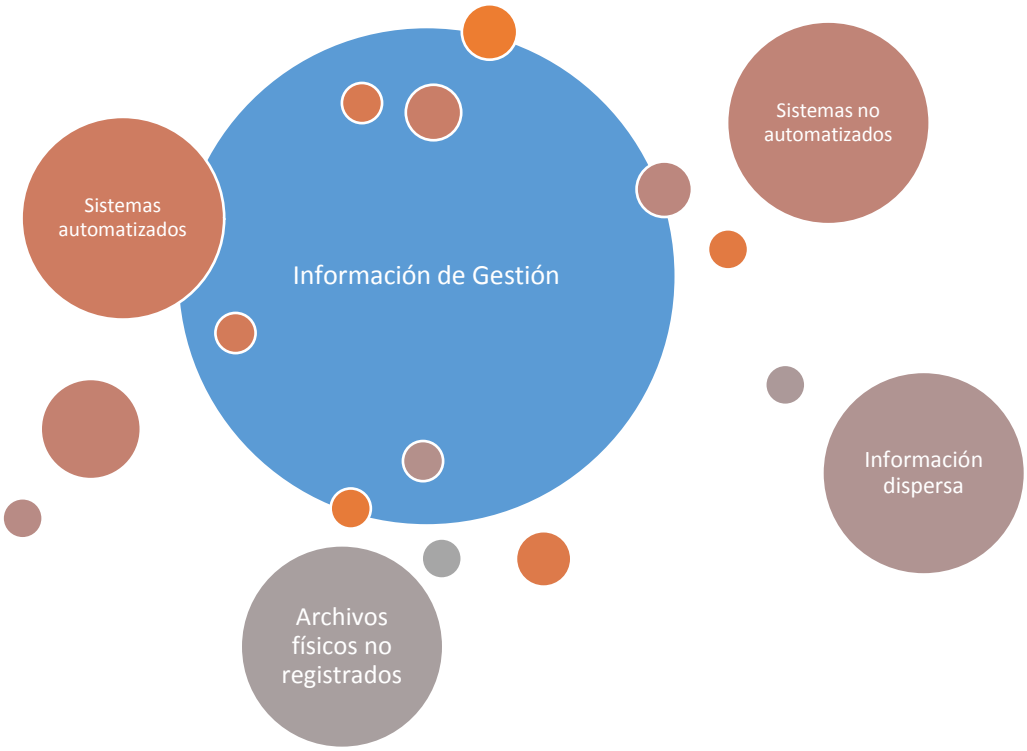


Diagrama Nro. 3: Esquematización de Información Institucional de la FGE. Fuente: Elaborado por el autor.

Para analizar la situación actual de la FGE, se utilizará una metodología para evaluación de Riesgos, particularmente COSO, donde se podrá realizar un diagrama para denotar la necesidad de implementar un SGSI. Para este fin, vamos a utilizar una sección de los procesos presentes en la cadena de valor, el proceso denominado Servicio de Atención Integral.

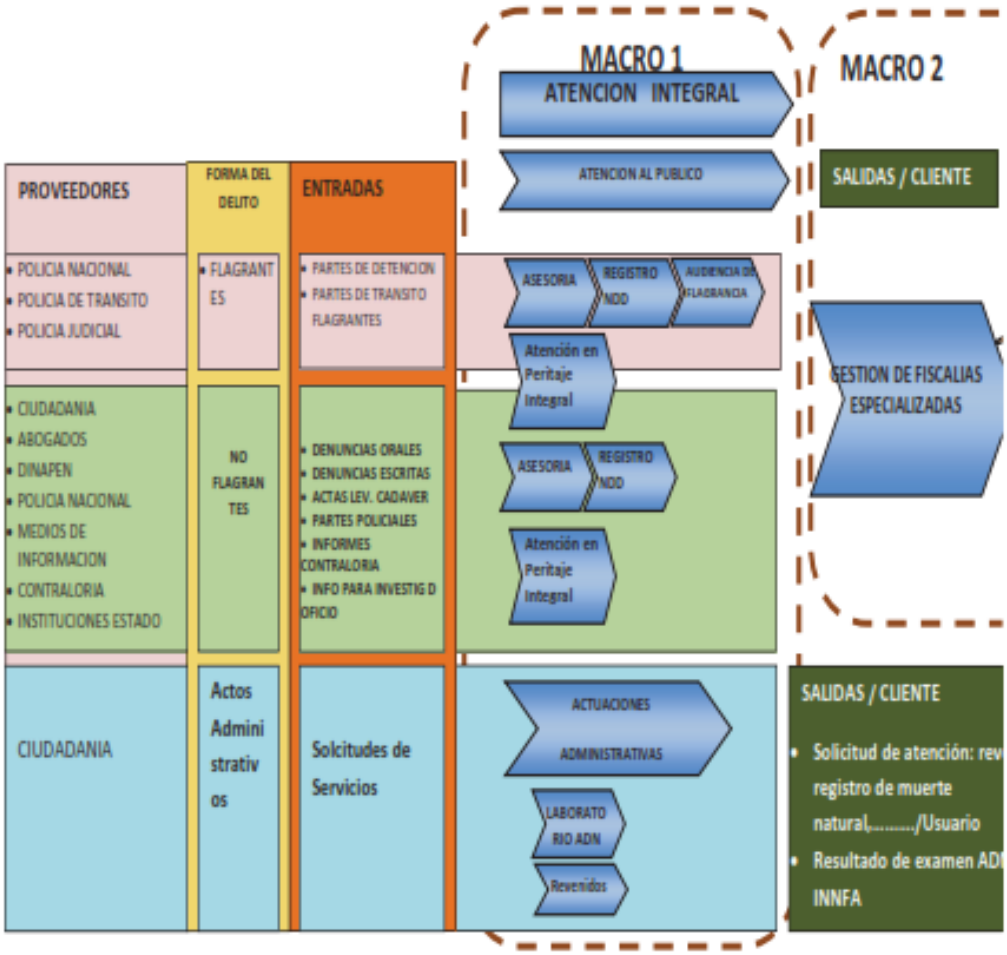


Diagrama Nro. 4: Mapa de procesos del Servicio de Atención Integral - FGE[8]

Para realizar un análisis de la situación actual de la institución, es necesario realizar una medición del riesgo de seguridad de la información, para este objetivo se realiza en dos partes, la primera que es un análisis de riesgo y la segunda que consiste en una evaluación del riesgo.

Definiciones generales relacionadas con la Evaluación de Riesgos

Eventos de Riesgo y oportunidades

Los eventos pueden catalogarse como positivos o negativos de acuerdo a su impacto, inclusive pueden presentarse con ambas categorías a la vez. Los eventos negativos se

[8]Fiscalía General del Estado – Estatuto Orgánico por Procesos – Internet: http://www.fiscalia.gob.ec/images/LOTAIP/A/Estatuto_Orgnico_por_Procesos_FGE.pdf - 29 de Marzo de 2013

determinan a la capacidad que tienen para erosionar o disminuir el valor que se agregan a los elementos que una organización produce y en el caso opuesto es por las nuevas oportunidades que se pueden generar a partir de los eventos ocurridos.

Los directivos son aquellos que dirigen o canalizan las oportunidades para que estas puedan ser incluidas en los objetivos de modo que puedan ser aprovechadas de la mejor manera.

Clasificación del riesgo

Se pueden clasificar los riesgos de las siguientes maneras:

- **Riesgos estratégicos:** Orientados básicamente a la administración de la organización y asuntos relacionados con la misión, visión y cumplimiento de objetivos estratégicos. Tareas encargadas generalmente a la alta gerencia.

- **Riesgos Operativos:** Orientados y relacionados con las áreas operativas y técnicas de una organización. Actualmente se observa la tendencia a incluir las deficiencias de los sistemas de información, modelos de gestión y descentralización desarticulada, produciendo ineficiencias y falta de compromiso en los objetivos de la institución.

- **Riesgos Financieros:** Orientados a los recursos de la entidad, incluyendo tareas de planificación y ejecución presupuestaria incluyendo estados financieros y bienes, del manejo claro y transparente depende el éxito en la ejecución de los proyectos.

- **Riesgos de cumplimiento:** Relacionados con el cumplimiento de requisitos legales, contractuales, éticos y el compromiso con las áreas a las que se debe, generalmente al público en general.

- **Riesgos de Tecnología:**Asociado a la capacidad de la organización para poner a disposición elementos tecnológicos que ayuden a satisfacer las necesidades inmediatas y futuras dentro de un plazo previsible para dar soporte al cumplimiento de los objetivos institucionales.

Metodologías para la Evaluación de riesgo

Mediante la metodología COSO para análisis y evaluación de riesgo, se analiza la situación general de la empresa u organización en las siguientes etapas:

- Identificación
- Medición
- Control
- Monitoreo.

Identificación de Riesgo

Cualquier organización, independientemente de su tamaño, organización interna, objetivos, etc se encuentra en permanente riesgo en distintas áreas, de hecho cualquier actividad que realizamos intrínsecamente contiene un componente de riesgo, que puede afectar la supervivencia o éxito en determinadas áreas.

En esta misma línea, se puede indicar que no es posible eliminar completamente el riesgo, pero es posible gestionarlo y determinar márgenes donde exista un riesgo aceptable para cada organización.

El primer paso para determinar los niveles de riesgo, es el describir clara y completamente los objetivos de la organización, debido a que estos son lo que serán afectados por los riesgos. En el caso de la Fiscalía General del Estado, se citan textualmente algunos temas relacionados con el objetivo principal de la institución, estos son:

“

…

Art. 2.- Visión

Ser una Institución que garantice el acceso a la justicia y el respeto de los Derechos

Humanos, con Talento Humano comprometido con el servicio a la ciudadanía, sin discriminación alguna, para mantener su confianza y credibilidad; apoyando el accionar latinoamericano en la lucha contra el crimen y la inseguridad.

Art. 3.- Misión

Dirigir la investigación pre-procesal y procesal penal, ejerciendo la acción pública con sujeción al debido proceso y el respeto de los Derechos Humanos, brindando servicios de calidad y calidez en todo el territorio nacional.

Art. 4.- Valores Corporativos

1. Ética	2. Transparencia	3. Compromiso
4. Lealtad	5. Creatividad	6. Liderazgo
7. Objetividad	8. Equidad	9. Responsabilidad Social

Art. 5.- Atribuciones y Responsabilidades de la Fiscalía General del Estado.-

1) Dirigir y promover, de oficio o a petición de parte, la investigación pre procesal y procesal penal, de acuerdo con el Código de Procedimiento Penal y demás leyes, en casos de acción penal pública; de hallar mérito acusar a los presuntos infractores ante el Juez competente e impulsar la acusación en la sustanciación del juicio penal, bajo los principios de oportunidad, objetividad y motivación;

2) Dirigir y coordinar las actuaciones de la Policía Judicial en las indagaciones previas y en las etapas del proceso penal;

3) Garantizar la intervención de la defensa de los imputados o procesados, en las indagaciones previas y en las investigaciones procesales por delitos de acción pública, quienes deberán ser citados y notificados para los efectos de intervenir en las diligencias probatorias y aportar pruebas de descargo, cualquier actuación que viole esta disposición carecerá de eficacia probatoria;

4) Ejercer durante el proceso penal, la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés

público y a los derechos de las víctimas, aplicando los postulados de economía procesal; accesibilidad, responsabilidad y complementariedad;

5) Dirigir, coordinar y supervisar las funciones de intercambio de la información y pruebas sobre nacionales o extranjeros implicados en delitos cometidos en el exterior, cuando así lo prevean los acuerdos y tratados internacionales;

6) Organizar y dirigir el Sistema Especializado Integral de Investigaciones;

7) Dirigir y coordinar el Sistema Nacional de Medicina Legal y Ciencias Forenses que contará con la ayuda de organismos gubernamentales y no gubernamentales con el fin de establecer, de manera técnica y científica, procedimientos estandarizados para la práctica de las pericias médico legales y su evaluación continua;

8) Conceder y revocar las correspondientes habilitaciones o acreditaciones, al personal de la Policía Judicial;

9) Expedir en coordinación con la Policía Nacional los manuales de procedimientos y normas técnicas para el desempeño de las funciones de la Policía Judicial;

10) Apoyar técnicamente a las personas que hacen sus prácticas pre profesionales en la Fiscalía General del Estado;

11) Organizar y dirigir el Sistema Nacional de Protección y Asistencia a Víctimas, Testigos y otros participantes en el proceso penal;

12) Apoyar y promover la implementación de políticas de seguridad ciudadana en coordinación con otras instituciones relacionadas con este tema;

13) Impulsar la celebración de convenios, acuerdos y procedimientos con organizaciones internacionales con el propósito de buscar asesorías, capacitación en temas jurídicos e investigativos;

14) Las demás determinadas en la Constitución y la ley.

Art. 6.- Objetivos Estratégicos Generales

1. Coadyuvar al fortalecimiento del proceso de reforma de la administración de la justicia emanado del mandato popular del 7 de mayo del 2011.

2. Actualizar, reorientar y potenciar el modelo de gestión, a partir del diseño y operación del nuevo estatuto organizacional por procesos.

3. Incluir y visibilizar el enfoque de derechos humanos en todos los procesos.

4. Reorientar el impulso a la lucha contra el crimen organizado a partir de modificaciones a introducir en los procedimientos, capacitación al talento humano y fortalecimiento de los servicios que presta la Fiscalía General del Estado.

5. Orientar la política institucional para garantizar una investigación objetiva que respete los derechos de las víctimas, ofendidos y procesados, en permanente observación del debido proceso.

6. Universalizar y globalizar la gestión para insertar prácticas internacionales conjuntas de la Fiscalía General del Estado, en el cumplimiento de la lucha contra el delito.

7. Promover enfoques de prevención con otras instituciones, a partir de la coordinación, articulación y complementariedad interinstitucional.

8. Reducir proactivamente los niveles de impunidad existentes, facilitando el acceso territorial a la administración de justicia.

9. Garantizar el acceso a la justicia en forma transparente, equitativa, incluyente, eficiente y desconcentrada, con un enfoque de servicio a la ciudadanía.

10. Implementar un plan de mejora continua de procesos internos en busca de la calidad, efectividad, transparencia, productividad y competitividad.

11. Formular e implantar un sistema de evaluación y control sobre la base de las leyes y la normativa institucional.

12. Garantizar la capacitación, metodologías y herramientas para la participación ciudadana a fin de lograr una gestión pública transparente eficiente y eficaz.

13. Orientar la gestión institucional a la obtención de resultados y a la optimización de recursos sobre la base del funcionamiento de un sistema de planificación.

14. Optimizar los recursos institucionales, manteniendo una estructura organizacional que evite su crecimiento desordenado, asegurando su evolución y dinámica de manera consistente y coherente a nivel nacional.

15. Fortalecer el trabajo en equipo, orientar los procesos al usuario del servicio, generar compromiso y empoderamiento del talento humano en su puesto de trabajo para lograr mayor productividad y eficacia.

„[9]

Complementando los criterios anteriormente indicados, que la mencionada incertidumbre puede ser generando también por factores externos a los que no tenemos control, como por ejemplo cambios en la tecnología, efectos globalizadores en ciertas áreas, reestructuración interna, cambio de autoridades (principalmente en el sector público), competencias y regulaciones, además de factores internos como malos empleados o corrupción, elecciones estratégicas, deficiencias en la asignación de recursos, etc. No obstante, la incertidumbre nace también de la imposibilidad de definir o precisas con exactitud la probabilidad de que se presente un evento que perjudique el diario desenvolvimiento de las actividades de la organización, además del impacto que este evento pueda ocasionar.

El valor que se agrega a cada actividad es generado, mantenido o eliminado por las descripciones de los administradores o directivos de cada área desde el planteo de o los proyectos pasando por su planificación hasta la ejecución diaria.

“La creación de valor ocurre por la asignación de recursos, incluyendo personal, capital, tecnología, y marca, donde el beneficio derivado es mayor que los recursos utilizados. La preservación de valor ocurre cuando el valor creado es sostenido en el tiempo, a través de calidad superior del producto o servicio, capacidad de producción, satisfacción al cliente, entre otras. El valor puede ser erosionado cuando estos objetivos no son alcanzados debido a una pobre estrategia o a su débil ejecución.

[9]Fiscalía General del Estado – Estatuto Orgánico por Procesos – Internet: http://www.fiscalia.gob.ec/images/LOTAIP/A/Estatuto_Orgnico_por_Procesos_FGE.pdf - 29 de Marzo de 2013

El valor es maximizado cuando la administración fija estrategias y objetivos para poner un balance óptimo entre objetivos de crecimiento, retorno y riesgos relacionados, y despliega eficiente y eficazmente los recursos en búsqueda de los objetivos de la entidad."[10]

FUENTES DE RIESGO	RIESGO	DECLARACIÓN DE RIESGO	
		CONDICIÓN	CONSECUENCIA
Administración de Redes e Infraestructura	Interrupciones en comunicaciones	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país
	Topología de red incorrecta	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional
	Mal dimensionamiento de las necesidades institucionales	Sub dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	Servicio lento y deficiente.
			Poco control sobre las actividades que se realizan en esos puntos.
			Se asocia a un mal servicio en general de toda la institución
	Capacitación del personal	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión
	Disponibilidad de Recurso humano	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional

[10]PCW - COSO II - El Enfoque Integrado para la Administración Corporativa de Riesgos Enterprise Risk Management - Integrated Framework - http://www.pwc.com/cl/es/cursos/finanzas-y-analisis-cuantitativo/coso-ii-enfoque-para-administracion-corporativa-de-riesgos.jhtml . Acceso: 19-04-2013

	Áreas Físicas para Data Center	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	Interrupción del servicio y daño físico en el equipamiento de servidores y equipos de comunicación.
	Conexión a internet	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	Los sistemas misionales de la FGE se encuentran desarrollados para que sean accedidos por internet, por lo que al disponer de un servicio itinerante dificulta el ofrecimiento de servicios a los usuarios
	Central Telefónica	Equipamiento, infraestructura y recursos insuficientes	La comunicación telefónica es inexistente en algunos lugares, los servicios no son centralizados, dificultando las actividades de gestión de los funcionarios en puntos remotos del país.
Administración de Equipos, Soporte al Usuario y Mantenimiento	Equipos de cómputo para usuarios internos	Equipamiento obsoleto o inexistente en los puntos de atención	Descontento por la inequidad en la atención de los requerimientos de los usuarios internos
			Lentitud en los procesos de atención al usuario
			Manejo discrecional de los procesos oficiales para atención al público y fiscalía especializada.
	Equipamiento de servidores para uso institucional	Equipamiento insuficiente y de distintas generaciones	Sistemas no funcionan de manera óptima, con bajo nivel de procesamiento, sumado a un creciente número de instituciones que consumen información de la FGE decrementa el nivel de satisfacción sobre el uso de las herramientas informáticas para los usuarios internos y externos,
	HelpDesk	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	Falta de retroalimentación para procedimientos de mejora
			Discrecionalidad o inatención a las demandas del usuario

			Retraso en la atención del usuario externo
			Falta de métricas de rendimiento por analista a cargo de las distintas áreas de soporte al usuario
	Información de usuarios internos	Información para el control y monitoreo de actividades del usuario imprecisa	Perfiles y acceso de usuario inadecuados para recursos sensibles.
			Información desactualizada e incompleta
	Catálogo de equipos	Catálogo de equipos manejado manualmente	Información imprecisa y desactualizada de catálogos es remitida periódicamente por los analistas provinciales en hojas electrónicas para que sea condensada en Quito
Desarrollo de aplicaciones	Respaldos de Base de Datos	Cronograma de respaldos inapropiado o con errores	Procedimientos de auditoría incompletos
			En caso de fallos críticos no se puede recuperar toda la información ingresada por los usuarios internos
			Impacto social debido a la sensibilidad de la información
	Aplicativos	Aplicativos con fallas o sin procesos de validación apropiados	Errores en el procesamiento o errores que imposibilitan el uso regular de los servicios de la institución
		Aplicativos o actividades no automatizadas	Información registrada manualmente y sin control sobre esos procedimientos
		Falta de capacitación a los usuarios en los aplicativos misionales	usuarios no utilizan los aplicativos de forma apropiada generando errores en las estadísticas de atención al usuario
Procesos de documentación	Varios sistemas de documentación	Información y manuales insuficientes	Sistemas poco difundidos y usados discrecionalmente

		Distintos responsables para esas áreas	No existe un responsable claro para dar soporte a los usuarios y gestiona miento de capacitación y garantías.
Procesos de Archivo	Sistemas de archivos manuales o inexistentes	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	Dificultad para acceder a la información de los expediente ingresados al Archivo central
	Personal insuficiente	Muchas variables necesarias para registrar las actividades de los fiscales	Lentitud en el proceso de registro de los expedientes que se van a ingresar a los distintos archivos.
Procesos de estadísticas	Estadísticas incoherentes	Metodologías de interpretación estadísticas dispares o incorrectas	Análisis criminológico inexacto
			Pérdida de credibilidad en las instituciones del sector justicia
			Mala percepción del trabajo de los funcionarios judiciales

Tabla Nro. 5 : Tabla de Riesgos presentes y consecuencias identificadas en la FGE

Medición de riesgo

Se debe calificar cada uno de los Riesgos según la matriz de acuerdo a las siguientes especificaciones: Probabilidad Alta se califica con 3, Probabilidad Media con 2 y Probabilidad Baja con 1, de acuerdo al número de veces que se presenta o puede presentarse el riesgo. Y el Impacto si es Leve con 5, si es Moderado con 10 y si es Catastrófico con 20. Esta métrica de definición de Probabilidad e Impacto, está propuesta en el documento denominado "MANUAL DE RIESGOS"[11] de la Alcaldía

[11] López, Luz Elena. Manual de Riesgo. Internet. http://puertonarino-amazonas.gov.co/apc-aa-files/36333937326664373030326136633438/Microsoft_Word___MANUAL_DE_RIESGOS.pdf Acceso: 18/04/2013.

de Nariño, sin embargo en la bibliografía consultada se presentaban otros posibles rangos para el cálculo de la Vulnerabilidad donde los valores podía oscilar entre 0 y 100 ó 0 y 70 en el campo de Impacto y valores en 0 y 50 para Probabilidad independientemente de los objetivos del estudio del análisis y valoración del riesgo. No obstante el procedimiento para el cálculo de la vulnerabilidad, mapa de riesgos, etc son los mismos que las otras metodologías, únicamente cambiaban los rangos para determinar el nivel de impacto y probabilidad.

Mapa de Riesgos

PROBABILIDAD								
	3	ALTA	MODERADO	V=15	IMPORTANTE	*V*=30	INACEPTABLE	*V*=60
	2	MEDIA	*TOLERABLE*	*V=10*	MODERADO	*V*=20	IMPORTANTE	*V*=40
	1	BAJA	ACEPTABLE	V=5	TOLERABLE	V=10	MODERADO	*V*=20
			LEVE		MODERADO		ALTO	
			5		10		20	
			IMPACTO					

Diagrama Nro. 5: Mapa de Riesgos y Matriz de Medición (Calificación y Evaluación). Fuente: Elaborado por el autor en base a la documentación obtenida del "Manual de Riesgos"[12].

Función de Vulnerabilidad

Nivel de riesgo o Vulnerabilidad = función de (probabilidad x impacto)

$$V = P \times I$$

Donde:

[12] López, Luz Elena. Manual de Riesgo. Internet. http://puertonarino-amazonas.gov.co/apc-aa-files/36333937326664373030326136633438/Microsoft_Word___MANUAL_DE_RIESGOS.pdf Acceso: 18/04/2013.

V= Vulnerabilidad

P = Probabilidad

I = Impacto

Lista Maestra de Riesgos

FUENTES DE RIESGO	RIESGO	ID	DECLARACIÓN DE RIESGO		PROBABILIDAD	IMPACTO	VALOR PROB.	VALOR IMPACTO	V
			CONDICIÓN	CONSECUENCIA					
Administración de Redes e Infraestructura	Interrupciones en comunicaciones	1	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país	ALTA	MODERADO	3	10	30
	Topología de red incorrecta	2	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional	ALTA	ALTO	3	20	60
	Mal dimensionamiento de las necesidades institucionales	3	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	Servicio lento y deficiente.	ALTA	MODERADO	3	10	30
				Poco control sobre las actividades que se realizan en esos puntos.					
				Se asocia a un mal servicio en general de toda la institución					
	Capacitación del personal	4	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión	MEDIA	MODERADO	2	10	20
	Disponibilidad de Recurso humano	5	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional	ALTO	MODERADO	3	10	40
	Áreas Físicas para Data Center	6	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	Interrupción del servicio y daño físico en el equipamiento de servidores y equipos de comunicación.	BAJA	ALTO	1	20	20

	Conexión a internet	7	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	Los sistemas misionales de la FGE se encuentran desarrollados para que sean accedidos por internet, por lo que al disponer de un servicio itinerante dificulta el ofrecimiento de servicios a los usuarios	ALTO	ALTO	3	20	60
	Central Telefónica	8	Equipamiento, infraestructura y recursos insuficientes	La comunicación telefónica es inexistente en algunos lugares, los servicios no son centralizados, dificultando las actividades de gestión de los funcionarios en puntos remotos del país.	BAJA	MEDIA	1	10	10
Administración de Equipos, Soporte al Usuario y Mantenimiento	Equipos de cómputo para usuarios internos	9	Equipamiento obsoleto o inexistente en los puntos de atención	Descontento por la inequidad en la atención de los requerimientos de los usuarios internos Lentitud en los procesos de atención al usuario Manejo discrecional de los procesos oficiales para atención al público y fiscalía especializada.	MEDIA	ALTO	2	20	40
	Equipamiento de servidores para uso institucional	10	Equipamiento insuficiente y de distintas generaciones	Sistemas no funcionan de manera óptima, con bajo nivel de procesamiento, sumado a un creciente número de instituciones que consumen información de la FGE en decremento el nivel de satisfacción sobre el uso de las herramientas informáticas para los usuarios internos y externos,	ALTA	ALTO	3	20	60

	HelpDesk	11	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	Falta de retroalimentación para procedimientos de mejora Discrecionalidad o inatención a las demandas del usuario Retraso en la atención del usuario externo Falta de métricas de rendimiento por analista a cargo de las distintas áreas de soporte al usuario	ALTA	MODERADO	3	10	30
	Información de usuarios internos	12	Información para el control y monitoreo de actividades del usuario imprecisa	Perfiles y acceso de usuario inadecuados para recursos sensibles. Información desactualizada e incompleta	ALTA	LEVE	3	5	15
	Catálogo de equipos	13	Catálogo de equipos manejado manualmente	Información imprecisa y desactualizada de catálogos es remitida periódicamente por los analistas provinciales en hojas electrónicas para que sea condensada en Quito	MEDIA	MODERADO	2	10	20
Desarrollo de aplicaciones	Respaldos de Base de Datos	14	Cronograma de respaldos inapropiado o con errores	Procedimientos de auditoría incompletos En caso de fallos críticos no se puede recuperar toda la información ingresada por los usuarios internos Impacto social debido a la sensibilidad de la información	MEDIA	ALTO	2	20	40

	Aplicativos	15	Aplicativos con fallas o sin procesos de validación apropiados	Errores en el procesamiento o errores que imposibilitan el uso regular de los servicios de la institución	MEDIA	ALTO	2	20	40
		16	Aplicativos o actividades no automatizadas	Información registrada manualmente y sin control sobre esos procedimientos	ALTA	MODERADO	3	10	30
		17	Falta de capacitación a los usuarios en los aplicativos misionales	usuarios no utilizan los aplicativos de forma apropiada generando errores en las estadísticas de atención al usuario	BAJA	MODERADO	1	10	10
Procesos de documentación	Varios sistemas de documentación	18	Información y manuales insuficientes	Sistemas poco difundidos y usados discrecionalmente	MEDIA	MODERADO	2	10	20
		19	Distintos responsables para esas áreas	No existe un responsable claro para dar soporte a los usuarios y ejecución de procesos de capacitación y garantías.	ALTA	MODERADO	3	10	30
Procesos de Archivo	Sistemas de archivos manuales o inexistentes	20	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	Dificultad para acceder a la información de los expediente ingresados al Archivo central	MEDIA	ALTO	2	20	40
	Personal insuficiente	21	Muchas variables necesarias para registrar las actividades de los fiscales	Lentitud en el proceso de registro de los expedientes que se van a ingresar a los distintos archivos.	MEDIA	ALTO	2	20	40
Procesos de estadísticas	Estadísticas incoherentes	22	Metodologías de interpretación estadísticas dispares o incorrectas	Análisis criminológico inexacto	ALTA	ALTO	3	20	60
				Pérdida de credibilidad en las instituciones del sector justicia					
				Mala percepción del trabajo de los funcionarios judiciales					

Tabla Nro. 6: Lista Maestra de Riesgos. Autor: Elaborado por el autor

Niveles de Vulnerabilidad

De acuerdo con los cálculos de los niveles de vulnerabilidad

ID	RIESGO	DECLARACIÓN DE RIESGO		P	I	V	NIVEL DE VULNERABILIDAD
		CONDICIÓN	CONSECUENCIA				
1	Interrupciones en comunicaciones	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país	3	10	30	IMPORTANTE
2	Topología de red incorrecta	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional	3	20	60	INACEPTABLE
3	Mal dimensionamiento de las necesidades institucionales	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de	Servicio lento y deficiente.	3	10	30	IMPORTANTE
			Poco control sobre las actividades que se				

		recepción fuera de la capital provincial	realizan en esos puntos. Se asocia a un mal servicio en general de toda la institución				
4	Capacitación del personal	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión	2	10	20	MODERADO
5	Disponibilidad de Recurso humano	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional	3	10	40	IMPORTANTE
6	Áreas Físicas para	Áreas destinadas para este efecto sin la	Interrupción del servicio y daño físico en el	1	20	20	MODERADO

	Data Center	seguridad y equipamiento necesario.	equipamiento de servidores y equipos de comunicación.				
7	Conexión a internet	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	Los sistemas misionales de la FGE se encuentran desarrollados para que sean accedidos por internet, por lo que al disponer de un servicio itinerante dificulta el ofrecimiento de servicios a los usuarios	3	20	60	INACEPTABLE
8	Central Telefónica	Equipamiento, infraestructura y recursos insuficientes	La comunicación telefónica es inexistente en algunos lugares, los servicios no son centralizados, dificultando las actividades de gestión de	1	10	10	TOLERABLE

			los funcionarios en puntos remotos del país.				
9	Equipos de cómputo para usuarios internos	Equipamiento obsoleto o inexistente en los puntos de atención	Descontento por la inequidad en la atención de los requerimientos de los usuarios internos Lentitud en los procesos de atención al usuario Manejo discrecional de los procesos oficiales para atención al público y fiscalía especializada.	2	20	40	IMPORTANTE
10	Equipamiento de servidores para uso institucional	Equipamiento insuficiente y de distintas generaciones	Sistemas no funcionan de manera óptima, con bajo nivel de procesamiento, sumado a un creciente número de instituciones que consumen	3	20	60	INACEPTABLE

			información de la FGE en decrementodel nivel de satisfacción sobre el uso de las herramientas informáticas para los usuarios internos y externos,				
11	HelpDesk	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	Falta de retroalimentación para procedimientos de mejora	3	10	30	IMPORTANTE
			Discrecionalidad o inatención a las demandas del usuario				
			Retraso en la atención del usuario externo				
			Falta de métricas de rendimiento por analista				

			a cargo de las distintas áreas de soporte al usuario				
12	Información de usuarios internos	Información para el control y monitoreo de actividades del usuario imprecisa	Perfiles y acceso de usuario inadecuados para recursos sensibles. Información desactualizada e incompleta	3	5	15	MODERADO
13	Catálogo de equipos	Catálogo de equipos manejado manualmente	Información imprecisa y desactualizada de catálogos es remitida periódicamente por los analistas provinciales en hojas electrónicas para que sea condensada en Quito	2	10	20	MODERADO

14	Respaldos de Base de Datos	Cronograma de respaldos inapropiado o con errores	Procedimientos de auditoría incompletos	2	20	40	IMPORTANTE
			En caso de fallos críticos no se puede recuperar toda la información ingresada por los usuarios internos				
			Impacto social debido a la sensibilidad de la información				
15	Aplicativos	Aplicativos con fallas o sin procesos de validación apropiados	Errores en el procesamiento o errores que imposibilitan el uso regular de los servicios de la institución	2	20	40	IMPORTANTE
16		Aplicativos o actividades no	Información registrada manualmente y sin	3	10	30	IMPORTANTE

		automatizadas	control sobre esos procedimientos				
17		Falta de capacitación a los usuarios en los aplicativos misionales	Usuarios no utilizan los aplicativos de forma apropiada generando errores en las estadísticas de atención al usuario	1	10	10	TOLERABLE
18	Varios sistemas de documentación	Información y manuales insuficientes	Sistemas poco difundidos y usados discrecionalmente	2	10	20	MODERADO
19		Distintos responsables para esas áreas	No existe un responsable claro para dar soporte a los usuarios y encargado de gestionar	3	10	30	IMPORTANTE

			lacapacitación y garantías.				
20	Sistemas de archivos manuales o inexistentes	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	Dificultad para acceder a la información de los expediente ingresados al Archivo central	2	20	40	IMPORTANTE
21	Personal insuficiente	Muchas variables necesarias para registrar las actividades de los fiscales	Lentitud en el proceso de registro de los expedientes que se van a ingresar a los distintos archivos.	2	20	40	IMPORTANTE
22	Estadísticas incoherentes	Metodologías de interpretación estadísticas dispares o incorrectas	Análisis criminológico inexacto Pérdida de credibilidad en las instituciones del sector justicia	3	20	60	INACEPTABLE

			Mala percepción del trabajo de los funcionarios judiciales				

Tabla Nro. 7: Tabla de nivel de riesgos en relación al Mapa de Riesgos. Autor: Elaborado por el autor.

VALORACIÓN	CANTIDAD DE RIESGOS IDENTIFICADOS
INACEPTABLE	4
IMPORTANTE	11
MODERADO	5
TOLERABLE	2
ACEPTABLE	0
TOTAL	22

Tabla Nro. 8: Tabla resumen de nivel de vulnerabilidad de los riesgos identificados. Fuente: Elaborado por el autor.

Control y Monitoreo

Las etapas de Control y Monitoreo serán explicadas, analizadas y desarrolladas en el capítulo II.

2. CAPÍTULO II – NORMA ISO 27001

2.1 Descripción general de la norma

La norma ISO – 27001 es un Estándar Internacional que ha sido elaborado para proporcionar un modelo definido para Establecer, Implementar, Operar, Monitorear, Revisar, Mantener, Mejorar un SGSI.

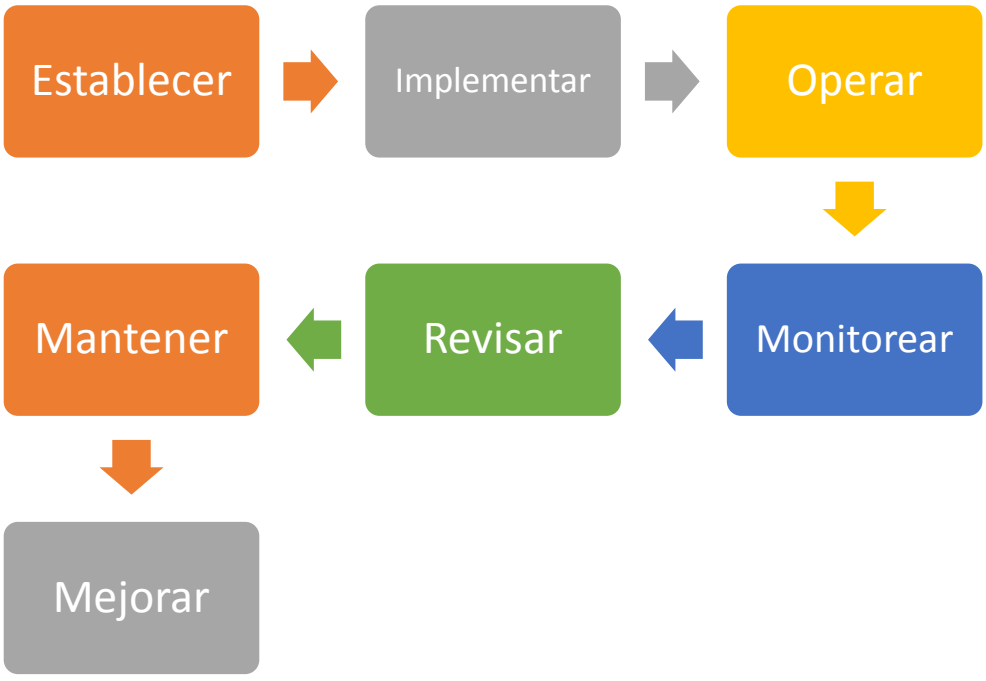


Diagrama Nro. 6: Esquematización del modelo para un SGSI. Fuente: Elaborado por el autor.

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Además este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

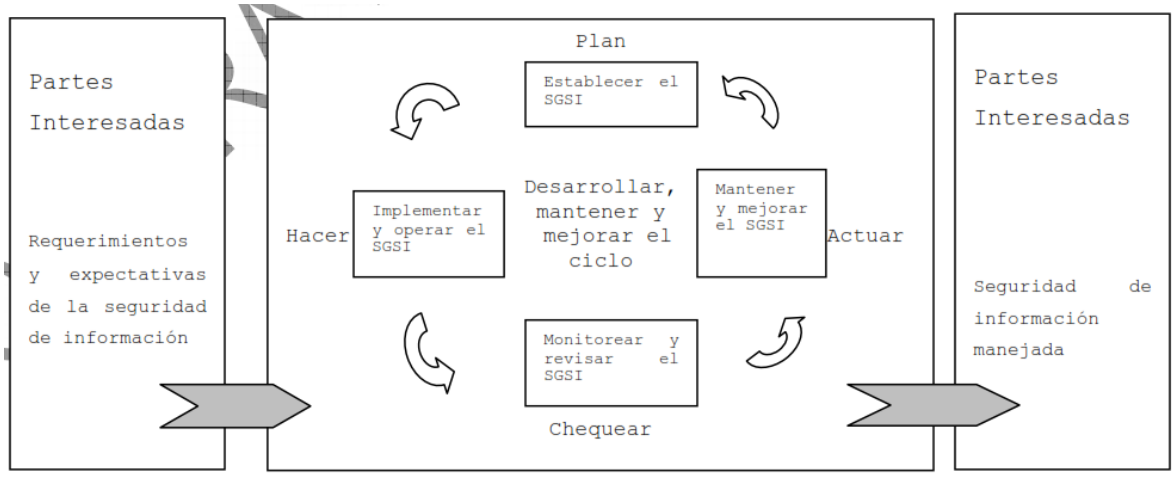


Diagrama Nro. 7: Esquematización de los procesos que actúan en un SGSI, adaptada al modelo por procesos PDCA.[13]

Planear **Establecer el SGSI**	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer **Implementar y operar el SGSI**	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y

[13] http://www.iso.org . ESTANDAR INTERNACIONAL – ISO / IEC 27001 – Primera Edición. www.iso.org. 18/06/2012

Monitorear y revisar el SGSI	experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar **Mantener y mejorar el SGSI**	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Tabla Nro.9: Descripción de PCDA, en concordancia con la Norma ISO 27001[14]

Plan: Establecer el SGSI

Posterior a definir el alcance del SGSI, en función al giro del Negocio, tipo de organización, localidad física, activos y tecnología es necesario incluir los detallar todos los componentes incluyendo la justificación de lo que fueron excluidos.

Demanda además definir políticas de seguridad:

Debe incluir marco general y objetivos de seguridad de la información

Requerimientos legales o contractuales relativos a la seguridad de la información

Estar en concordancia con el trasfondo estratégico de gestión de riesgos, que establecerá y dispondrá el SGSI

Debe estar socializado y aprobado por la directiva de la organización

Metodología de evaluación de riesgos, incluyendo los criterios. Para definir la metodología para la evaluación del riesgo, existen varias metodologías que pueden ser utilizadas, sin embargo es perfectamente factible que se realice una metodología propia.

Dentro de esta metodología se deben definir entre otras cosas, que activos se encuentran dentro del alcance del SGSI y los responsables directos o propietarios. (El

[14] http://www.iso.org . ESTANDAR INTERNACIONAL – ISO / IEC 27001 – Primera Edición. www.iso.org. 18/06/2012

término propietario se refiere a quien tiene el control para la producción, desarrollo, mantenimiento o uso, formalmente reconocido, no necesariamente a quien dispone de derechos de propiedad)

También se deben considerar:

- Definir e identificar las amenazas de los activos.
- Vulnerabilidades que pueden presentarse
- Impacto en la confidencialidad, integridad y disponibilidad
- Analizar de forma realista, la posibilidad de la ocurrencia de una falla de seguridad
- Estimar niveles de riesgo o aceptación de riesgo previamente establecidos, donde se presenta la posibilidad de que un riesgo aceptable o necesita ser tratado.

Establecer de forma coherente a los análisis anteriores un procedimiento o proceso para el Tratamiento de riesgos, donde se debe:

- Aplicar los controles adecuados
- Aceptar el riesgo, siempre y cuando estos sigan cumpliendo por los criterios de para aceptación de riesgos y las políticas anteriormente definidas.
- Evitar el riesgo, haciendo las gestiones necesarias para que se suspenda las actividades que originan este incidente.
- Transferir los riesgos a terceros, por ejemplo compañías aseguradoras, proveedores de outsourcing, etc.

Diagrama Nro. 8: Imagen descriptiva de la Gestión de riesgos propuesta por el portal web www.iso27000.es[15]

La norma cuenta con un conjunto de controles establecidos y enumerados en un anexo para el tratamiento del riesgo, sin embargo pueden incluirse otros controles que no se encuentren en la versión original de la normativa.

Con este insumo se debe realizar una Declaración de Aplicabilidad que incluya:

- Objetivos del control
- Controles seleccionados y los motivos por los cuales fueron elegidos.
- Objetivos de Controles ya implementados
- Controles excluidos de la selección para su aplicación, incluyendo los motivos por lo que no fueron incluidos
- Controles adicionales que no están incluidos formalmente en la norma.

[15] SGSI - ¿Cómo se implementa un SGSI? – Internet - http://www.iso27000.es/sgsi.html#section2d - Acceso: 15-04-2013

Do: Implementar y utilizar el SGSI

El planteamiento de un SGSI debe ser der forma clara, para que el tratamiento del riego pueda ser eficiente para así identificar las acciones, recursos, responsabilidades y prioridades de los riesgos a los que puede estar sometida la información.

Plantear de forma clara un plan de tratamiento de riesgos donde se encuentren identificados todas las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Para cumplir con este propósito es necesario el cumplir con los siguientes parámetros:

- Contar con un Plan para tratamiento de riesgos, para establecer de forma precisa los controles que serán requeridos, además de una asignación de recursos, responsabilidades y prioridades.
- Implementar los controle seleccionados de manera integral
- Establecer métricas de control para medir la eficiencia de las acciones tomadas, para que posteriormente puedan ser reproducibles y comparables; y posteriormente sean parte de una estadística confiable.
- Establecer y promover programas de socialización y capacitación que ayuden a la formación y facilite el cumplimiento de los temas relacionados con la seguridad de la información entre todos los empleados de la organización o institución.
- Gestionar las operaciones propias del SGSI
- Gestionar los recursos que sean necesarios para cumplir con las funciones de mantenimiento de la seguridad de la información.
- Establecer formalmente los procedimientos y esquema de controles necesarios que permitan una solución rápida a los incidentes de seguridad.

Check: Monitorizar y revisar el SGSI

Como parte de los procedimientos de control es necesario contar con actividades de monitoreo y revisión para:

- Detectar errores que pueden ser producidos por el procesamiento de información
- Identificar problemas o brechas de seguridad
- Conjuntamente con la directiva determinar y evaluar, las actividades realizadas y los resultados obtenidos han garantizado seguridad en la información, tanto a nivel de personal, procedimientos o dispositivos tecnológicos.
- Mediante indicadores previamente establecidos, detectar y prevenir eventos e incidentes de seguridad.
- Determinar si las acciones correctivas utilizadas en un incidente resolvieron el problema con efectividad.

Además la revisión de las tareas de forma periódica, con mediciones de eficacia y eficiencia del SGSI, vigilando con rigurosidad si continua con las políticas y objetivos por los que fue implementados, organizando y evaluando los resultados de las auditorias de seguridad que se han aplicado, tipos de incidentes reportados, sugerencias y observaciones de todos los actores implicados.

Establecer mediciones para la efectividad de cada uno de los controles implementados, con vigilancia que cumplan completamente los objetivos que se especificaron, además de establecer una planificación para le evaluación de:

- Riesgos previstos
- Riesgos residuales
- Niveles de aceptación de Riesgo

Todos estos tienen que estar enfocados en los cambios que se pueden presentar en la Tecnología, objetivos y procesos comerciales, Amenazas identificadas, Efectividad

delos controles implementados, Eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

Realizar auditorías internas periódicas para constatar el buen funcionamiento del SGSI

Permanente revisión del SGSI por parte de los directivos para determinar si los alcances planteados originalmente siguen siendo los más adecuados y que las mejoras que se implementan son efectivas y evidentes

Además las actividades de control, también abarcan la permanente actualización de los planes de seguridad en función de las observaciones, conclusiones o nuevos hallazgos encontrados durante las actividades de monitorización y revisión de los procesos y el mismo SGSI.

Controlar que todos los cambios o acciones sean registrados sobre eventos que puedan haber impactado en la efectividad del SGSI.

Act: Mantener y mejorar el SGSI

Se deben implantar en el SGSI las mejoras identificadas.

Realizar las acciones preventivas y correctivas adecuadas, y coordinar eventos para compartir las lecciones aprendidas de las experiencias propias y de otras organizaciones.

Establecer niveles de profundidad en las explicaciones o comunicaciones entre los interesados de acuerdo al detalle que se necesita cada parte para continuar con el proceso normal de sus actividades.

Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo.

La adopción de un SGSI debe ser una decisión estratégica para una organización, en este caso la Fiscalía General del Estado.Se considera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

La información, conjuntamente con los procesos y sistemas relacionados para el uso de ella, son activos muy valiosos de cualquier institución, el poder disponer de los elementos de la seguridad informática (confidencialidad, integridad y disponibilidad) constituye una parte esencial para mejorar o mantener los niveles de calidad, conformidad legal e imagen institucional y así lograr los objetivos y planes que la institución misma se ha propuesto.

Hoy en día existen muchas organizaciones con sistemas de información, tanto simples como sofisticados, pero que están expuestos sin discrimen a un número cada vez más elevado de amenazas que podrían aprovechar cualquier vulnerabilidad existente, donde pueden someter a ataques de activos críticos de información a diversas formas, como por ejemplo el fraude, espionaje, sabotaje, vandalismo, virus y gusanos informáticos, el “hacking” o los ataques de denegación de servicio entre muchos otros son amenazas cada más probables, además no se debe descartar la posibilidad de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

En el caso particular de la FGE, existen como en cualquier otra organización puntos débiles que no han sido completamente gestionados, las amenazas de virus informáticos, fallas de comunicaciones, sumada a la baja capacitación de la mayoría de los funcionarios, aumenta la severidad de una amenaza. Actualmente se dispone solamente de un analista en cada provincia (a excepción de Quito y Guayaquil), en donde al presentarse un incidente en cualquier cantón este funcionario debe trasladarse para gestionar problemas de todo tipo, tomando en muchos casos varios días de interrupción de servicio o utilizando metodologías alternas a manera de contingencia, que posteriormente tienen que ser gestionadas para que sean ingresadas al sistema

informático misional, lo que causa muchas veces confusión al usuario externo y molestias al usuario interno por el doble trabajo que se tiene que realizar.

Por otro lado y a razón de cumplir las normativas legales, adaptarse de forma dinámica y puntual a las condiciones siempre variables del entorno, la protección adecuada de los objetivos de negocio para asegurar la máxima satisfacción del usuario (generalmente víctimas de algún hecho presumiblemente delictivo, siendo estos en varios casos de tipo de violencia sexual o intrafamiliar y en otros pueden presentar algún tipo de lesion) y el aprovechamiento de nuevas tecnologías para mejora de los procesos relacionados con el giro de negocio (actualmente se pretende extender de manera generalizada el uso de firma electrónica para los procesos administrativos internos, expediente digital; y correspondencia, gestión de audiencias y comunicados oficiales), son algunos de los aspectos fundamentales en los que el SGSI que se plantea, corresponde a una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

La plataforma de infraestructura informática de la FGE es muy dispareja, abarca diferentes versiones de sistemas operativos, equipos informáticos muy viejos y de última tecnología, servidores de varias generaciones, sistemas centralizados sin contingencias o redundancia hacen difícil garantizar un nivel de protección aceptable, de hecho el intentar contar un sistema de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado.

Por tanto, el principal propósito de un sistema de gestión de la seguridad de la información es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Sin embargo, existen entidades que guardan estos conceptos, con la finalidad de acumular réditos económicos, en este caso en particular, la Fiscalía General del Estado, no realiza actividades de orden económico, pero salvaguarda intereses y bienes

jurídicos, que si son mal salvaguardados, representaría eventos de ilegalidad e inseguridad jurídica en todo el país, pudiendo esto desembocar en demandas que repercutirían sobre el personal técnico y jurídico de la institución.En nuestra normativa jurídica existen todavía muchos vacíos legales, debido principalmente a la rápida evolución de la tecnología y se suma a que nuestro Código Penal es antiguo y a veces inoperable e incompatible con esta nueva forma de delincuencia, facilitado en algunas ocasiones el poder cumplir completamente con la contraparte de salvaguardar la seguridad informática, que es la de controlar y atrapar a los llamados ciberdelincuentes.

En sí mismo, el SGSI que se plantea permite el cumplimiento de:

- Normativas legales (Constitución del Ecuador, Código Penal y de procedimiento Penal, Normativa internacional, convenios internacionales donde el país es sucriptor, etc) y buenas prácticas (gestión de incidentes, manejo de base de conocimiento, etc)

- Adaptación dinámica y puntual de las condiciones del entorno tecnológico, de inicio adaptado a un plan agresivo de mejoramiento de plataforma de Hardware y software, pero con la planificación y visión para que sea flexible para los futuros cambios que se podrían presentar tanto a nivel de atacante como de técnico responsable.

- Protección adecuada a los objetivos del negocio, que deben ser en algunos casos reformados desde la normativa interna y/o registro oficial, con la finalidad de asegurar el máximo beneficio y aprovechamiento de toda la información recolectada para generar políticas de prevención pública del delito, políticas anti delincuenciales y mejorar el sistema de justicia del país.

Diagrama Nro. 9: Imagen descriptiva de la interacción de los componentes de un SGSI con los riesgos, propuesta por el portal web www.iso27000.es[16]

"En general, en los medios técnicos, los niveles de seguridad es limitado e insuficiente, en vista de la dinámica tecnológica en la que nos desenvolvemos, sin embargo para dar cumplimiento efectivo en esta tarea es necesario el determinar un MODELO DE GESTION DE SEGURIDAD, donde se contemplen los procedimientos adecuados, además de la planificación e implementación de controles de seguridad basados en una EVALUACION DE RIESGOS anteriormente elaborada para disponer de una medición de eficacia de los mismo."[17]

En esquemas más generales, se establece que un SGSI debe concordar con los objetivos centrales de la institución además de establecer y definir, entre otras cosas, los procedimientos necesarios para mantener los riesgos en niveles bajos. En este último se refiere a que se debe conocer de la forma más clara posible los riesgos a los

[16] SGSI - ¿Cómo se implementa un SGSI? – Internet - Acceso: 15-04-2013 - http://www.iso27000.es/sgsi.html#section2d

[17] SGSI - ¿Para que sirve un SGSI? – Internet - Acceso: 15-04-2013 - http://www.iso27000.es/sgsi.html#section2b

que podría someterse su información; y como se ha indicado antes definir y documentar los procesos para el gestionamiento de incidentes de seguridad, que debe ser socializado y reconocido por todos los miembros de la institución y que debe estar en constante mejora.

En otras palabras, el enfoque del proceso para la gestión de la seguridad de la información pretende fomentar que sus usuarios enfaticen la importancia de:

“

- Entender los requerimientos de seguridad de la información de una organización y lanecesidad de establecer una política y objetivos para la seguridad de la información;
- Implementar y operar controles para manejar los riesgos de la seguridad de lainformación;
- Monitorear y revisar el desempeño y la efectividad del SGSI; y
- Mejoramiento continuo en base a la medición del objetivo.

„[18]

SGSI - Documentación

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

[18] http://www.iso.org . ESTANDAR INTERNACIONAL – ISO / IEC 27001 – Primera Edición. www.iso.org. Acceso: 18/06/2012

Diagrama Nro. 10 : Esquematización de los distintos niveles de documentación presentes en la norma ISO/IEC 27001. Autor: Varios autores

Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Está constituido por los siguientes aspectos:

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI. Se debe incluir una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del SGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Metodología de evaluación de riesgos: descripción de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada.

Plan de tratamiento del riesgo: documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implantar los controles necesarios para proteger la misma.

Declaración de aplicabilidad (SOA -Statement of Applicability-, en sus siglas inglesas): documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Procedimientos relativos al nivel 1: procedimientos que regulan cómo se realizan, gestionan y mantienen los documentos enumerados en el nivel 1.

Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información, además también describe como medir la efectividad de los controles.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

Control de la documentación

Todos los documentos requeridos por el SGSI serán protegidos y controlados.

Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

Aprobar documentos y prioridades o clasificación de empleo antes que estos sean emitidos.

Revisiones, actualizaciones y aprobaciones de documentos de forma periódica y programada.

Asegurar que los cambios y las revisiones de documentos sean identificados.

Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas en los departamentos correspondientes, de manera oportuna.

Asegurar que los documentos permanezcan legibles y fácilmente identificables.

Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.

Asegurar que los documentos de origen externo sean identificados.

Asegurar el control de la distribución de documentos.

Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

2.2 Correspondencia con el Sistema de Gestión de Calidad ISO 9001:2000

Entre los intereses principales de la institución se encontraba en certificar algunos procesos mediante la norma ISO/IEC 9001:2000. Este proceso fue iniciado con poca repercusión debido a que no se contaba con todos los procesos de socialización adecuados para generar la conciencia de documentación y procedimientos que se deben tomar para impulsar este importante paso en el desarrollo institucional.

Sin embargo, se prepararon e identificaron algunos procesos que tienen relación con la norma 27001 que se pretende aplicar en esta institución.

Sistema de gestión de calidad implementado bajo la norma ISO/IEC 9001 guarda mucha relación con la norma ISO/IEC 27001, de por si ambos utilizan los procedimientos PDCA (Plan, Do, Check, Act) desarrollado por Edwards Demming, que se traducen en las Fases de Planeación en donde se recogen los objetivos que se desean obtener, Fase de implementación que ejecuta los procedimientos necesarios para poner en funcionamiento la normativa, fase de revisión referente al permanente monitoreo de los objetivos que se plantearon y la fase de mejoras. Todas estas presentes en cualquiera de las dos normas.

En sí mismo los procesos referentes a calidad fueron utilizados como base para otros modelos, como seguridad de la información, medio ambiente, continuidad de negocio, etc, por lo tanto, si fueron implementados en la norma de calidad, pueden ser también utilizados en la norma de seguridad de la información.

Estos son algunos ejemplos de las concordancias de los modelos:

“

- Gestión de documentación: el procedimiento utilizado para la gestión de documentación en el SGC puede ser usado con el mismo objetivo en el SGSI, sólo con algunas pequeñas adaptaciones.

- Auditoría interna: se puede utilizar el mismo procedimiento para el SGC y para el SGSI; aunque la auditoría interna concreta generalmente sería realizada por personas diferentes, ya que no es muy probable que una misma persona conozca en profundidad tanto sobre seguridad de la información como sobre calidad.

- Medidas correctivas y preventivas: el procedimiento utilizado para el SGC puede ser usado con el mismo objetivo en el SGSI, aunque es probable que sean personas diferentes quienes resuelvan los temas relacionados con SGC o SGSI.

- Gestión de recursos humanos: el mismo ciclo de planificación, capacitación y evaluación de RR.HH. se utiliza para ambos sistemas de gestión; naturalmente, la diferencia radica en el perfil de capacidades y conocimientos requeridos.

- Revisión por parte de la gerencia: los principios de la revisión por parte de la gerencia son los mismos para ambos sistemas de gestión; aunque no sería recomendable realizar ambas revisiones en paralelo, la gerencia ya estará acostumbrada a tomar decisiones sobre el SGC; por lo tanto comprenderán mejor cómo tomar decisiones en el contexto del SGSI.

- Establecimiento de objetivos comerciales y seguimiento de su cumplimiento: se fija el mismo mecanismo en ambas normas; por eso, la gerencia estará acostumbrada a una planificación sistemática de este tipo.

„[19]

Información Técnica más detallada se puede encontrar en el Anexo C de la Norma ISO/IEC 27001.

3. CAPÍTULO III – APLICACIÓN DE LA NORMA ISO 27001

3.1 Aplicación de la Norma ISO 27001

Política de Seguridad

Para establecer una política de seguridad, se debe contar con anterioridad de un "Comité de Seguridad de Información" o un comité que realice las veces de este, para

[19]Kosutic, Dejan - Usar la ISO 9001 para implementar la ISO 27001 – Internet : http://blog.iso27001standard.com/es/2010/04/02/usar-la-iso-9001-para-implementar-la-iso-27001/ - Acceso : 25-04-2013

que pueda analizar, aprobar y coordinar los procesos de implementación de las políticas, controles y monitoreo del SGSI.

En este caso particular no se encuentra creado tal comité, por lo que el primer paso sería adaptar la estructura organizacional para contar con esta figura.

De hecho, de acuerdo a la bibliografía consultada, donde se incluye la LOSEP (Ley Orgánica del Sector Público del Ecuador), dicha figura no se encuentra contemplada, únicamente se menciona el "Comité de Gestión de Calidad de Servicio y desarrollo Institucional", con funciones no implícitas para esta labor que debe estar presente en cada institución del sector público.

"Art. 138.- Del Comité de Gestión de Calidad de Servicio y el Desarrollo Institucional.-En las instituciones establecidas en el artículo 3 de la LOSEP, se integrará el Comité de Gestión de Calidad de Servicio y el Desarrollo Institucional que tendrá la responsabilidad de proponer, monitorear y evaluar la aplicación de las políticas, normas y prioridades relativas al mejoramiento de la eficiencia institucional.

El Comité tendrá la calidad de permanente, y estará integrado por:

a) La autoridad nominadora o su delegado, quien lo presidirá;

b) El responsable del proceso de gestión estratégica;

c) Una o un responsable por cada uno de los procesos o unidades administrativas; y,

d) La o el responsable de la UATH o quien hiciere sus veces.

En las unidades o procesos desconcentrados se contará con comités locales los cuales serán permanentes y deberán coordinar sus actividades con el comité nacional.

„[20]

Además la normativa relacionada con la Contraloría General del Estado hace recomendaciones para la creación de Unidades de Seguridad Informática (circunscrita a

[20]LOSEP - http://www.finanzas.gob.ec/wp-content/uploads/downloads/2013/01/REGLAMENTO_LEY_SERVICIO_PUBLICO1.pdf .Reglamento de la Ley Orgánica del Sector Público del Ecuador Acceso:22/04/2013

la unidad o dirección de Tecnologías de la Información), más no se establece lineamientos claros sobre el tratamiento de la seguridad de la información como tal, en un esquema de trabajo de un SGSI o similar.

Se redacta una política de seguridad en función de lo que este momento se encuentra vigente, para que sea aprobado desde el Comité de Gestión de Calidad de Servicio y Desarrollo Institucional, sin embargo las funciones de este, no se encuentran definidas con la especificidad del caso, no obstante se encuentran descrita la función de: "… tendrá la responsabilidad de proponer, monitorear y evaluar la aplicación de las políticas, normas y prioridades relativas al mejoramiento de la eficiencia institucional."[21] Enfocada más hacia el área del control de calidad que al de seguridad de la Información, pero abre la puerta a la posibilidad de poder iniciar este procedimiento.

Redacción de Política de Seguridad

La redacción del documento de Políticas de Seguridad, constituye un trabajo que tratará de plasmar todos los responsables, tareas, controles y formas de medición para un SGSI.

Existen responsables de su aprobación como se mencionó en las secciones anteriores y debe contener referencias hacia:

1. Estudiar los requisitos: Relacionada con revisión general de la normativa legal, reglas corporativas, normativa existente, etc. Además de la norma ISO/IEC 27001

2. Tomar en cuenta los resultados de su evaluación de riesgos: Identificar que temas y en qué medida se deben abordar las políticas de seguridad

[21]Fiscalía General del Estado – Estatuto Orgánico por Procesos – Internet: http://www.fiscalia.gob.ec/images/LOTAIP/A/Estatuto_Orgnico_por_Procesos_FGE.pdf - 29 de Marzo de 2013

3. Optimizar y alinear sus documentos: Reconocer, organizar e incluir los documentos relacionados realizados con anterioridad, para no generar normas repetitivas, redundantes o contradictorias con la nueva política.

4. Estructurar el documento: Realizar un documento en función de la normativa documental que se posee. Una distribución de contenidos dentro de este documento puede ser:

    a. Introducción

        i. Objetivos

        ii. Alcances y Limitaciones

        iii. Definiciones

    b. Responsabilidades Generales

    c. Adhesión a la Política

    d. Protección de la Información

    e. Apoyo Dirección Ejecutiva

    f. Clasificación de la Información

    g. Uso de Activos de Información

    h. Normas que componen la Política[22]

5. Redactar el documento: Realizar un documento con lenguaje sencillo y de alto nivel para que pueda ser captado por toda la comunidad a la que está enfocada

6. Conseguir la aprobación del documento: Debe ser presentado ante la alta directiva para que esta pueda impulsar el proyecto a toda la organización

[22] Servicio de Gobierno Regional de Magallanes y Antártica Chilena - Política de Seguridad de la información – Internet: http://164.77.209.178/sitioweb2011/archivos/RESGR132_2011.pdf – Acceso: 23/04/2013

7. Capacitación y concienciación de sus empleados: Distribuir estas directrices con capacitación, indicando las ventajas de esta política frente a otras realizadas anteriormente.[23]

Documento de Política de Seguridad para la FGE

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION[24]

FISCALIA GENERAL DEL ESTADO

NOTA DE CONFIDENCIALIDAD

El presente documento contiene información que pertenece a la Fiscalía General del Estado de la República del Ecuador, que ha sido elaborado con el propósito general de impulsar, asegurar y preservar las actividades operacionales de la misma, a nivel administrativo y misional, este documento no puede ser entregado o revelado, parcial o totalmente a terceras partes sin la autorización del Comité de Seguridad de la Información (Comité de Gestión de Calidad de los Servicios y desarrollo Institucional)

Firmas de los responsables.

ELABORADO POR	REVISADO POR	APROBADO POR

[23]Kosutic, Dejan – Siete Pasos para implementar políticas y procedimientos – Internet : http://blog.iso27001standard.com/es/tag/politica-de-seguridad-de-la-informacion/ - Acceso: 23/04/2013
[24]Formato general para redacción de Políticas de Seguridad de la Información – Internet: https://docs.google.com/viewer?url=http%3A%2F%2Fwww.dipres.gob.cl%2F572%2Farticles-51683_intro_anexo5.doc – Acceso: 22/04/2013

_ _ _ _ _ _ _ _ _ _ _ _ _ _	_ _ _ _ _ _ _ _ _ _ _ _ _ _	_ _ _ _ _ _ _ _ _ _ _ _ _ _

INDICE

[25] Servicio de Gobierno Regional de Magallanes y Antártica Chilena - Política de Seguridad de la información – Internet: http://164.77.209.178/sitioweb2011/archivos/RESGR132_2011.pdf – Acceso: 23/04/2013

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN								
Nº Revisión	**Fecha de presentación**	**Fecha Aprobación**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**	**Dirección Administrativa**	**Aprobado por**	**Observaciones**
0(Cero)			Elaboración inicial	Todas				
1								
2								
3								

Introducción

Objetivos

Las políticas presentadas en este documento tienen como objetivo:

- Establecer de forma clara y apropiada los mecanismos que ayuden a garantizar la seguridad de los activos relacionados con la información para la Fiscalía General del Estado.
- Representar los intereses de los Directivos y responsables de las distintas áreas de servicio, en relación a la administración y utilización de los activos de información de la institución por parte de los usuarios internos y externos.
- Indicar las medidas a adoptarse para la protección de los activos de información
- Establecer una cultura de seguridad de la información en la institución, dirigida hacia todos los funcionaros que prestan servicios en la FGE.
- Especificar las medidas de seguridad de la información para proteger de manera óptima contra amenazas que puedan afectar la confidencialidad, integridad y disponibilidad ocasionando:
    - Pérdida o uso inapropiado de los activos de información de la institución
    - Corrupción
    - Pérdida o uso inapropiado de información sensible
- Socializar en la FGE, lineamientos que garanticen la incorporación de las actividades apropiadas que guardan relación con la seguridad de la información.

Alcance

Esta política es de uso y aplicación obligatoria para todas las personas que laboran en la Fiscalía General del Estado de la República del Ecuador, en cualquier modalidad de trabajo sean estos de nombramiento provisional, nombramiento definitivo, modalidades de contrato, calidad de Servicios, etc, incluyendo a personal de terceras empresas,

pertenezcan estas al Sector Público o Sector Privado, aunque no presten actividades de servicio misional.

Actúa sobre todos los activos de información que dispone la institución, tanto anteriores, actuales o futuros, de forma tal que aunque no se indique explícitamente no constituye un requisito excluyente para no resguardar dicho activo de información.

La política cubre toda la información impresa o escrita en cualquier medio o almacenado mediante cualquier forma electrónica o magnética u óptica o digital o transmitida por correo electrónico o mediante algún método telemático, relacionada con documentos o videos o elementos de audio o imágenes o similares.

La política se basa en el contenido incluido en la norma ISO/IEC 27001 y de los requisitos legales, administrativos, normativos y contractuales referentes a la seguridad de la información, que sean aplicables o propiedad de la institución.

La presente política entra en rigor desde la fecha de suscripción por parte del Comité de Seguridad de la Información (Comité de Gestión de Calidad de Servicio y Desarrollo Institucional).

Definiciones

A continuación se indica un conjunto de definiciones y su conceptualización en el contexto de seguridad de la información con la finalidad de unificar criterios y asegurar un mejor cumplimiento de la presente política:

Activo de Información: Elementos relevantes en las etapas de producción, distribución, comunicación, visualización y afines a los procesos que agregan valor para la institución.

Confidencialidad: Propiedad referente al acceso restringido para quienes tienen autorización a los activos de información.

Continuidad del negocio: Estado en el cual las operaciones relacionadas estrechamente con el giro del negocio de la organización continúan ininterrumpidas

Disponibilidad: Propiedad mediante la cual se garantiza que los activos permanecen accesibles para quienes tienen las autorizaciones de acceso.

Documentos Públicos: Documentación al que tiene acceso sin restricciones o que no está categorizado como reservado o secreto.

Documento Reservado: Documentación categorizada con la categoría de reservada o clasificada, destinada a una unidad o persona en particular a razón de una normativa legal o administrativa que confiere dicha categoría.

Incidente de seguridad: Situación que se presenta en procesos particulares, concretamente en lo referente a la seguridad de la información y que puede comprometer negativamente las actividades que agregan valor a la organización.

Integridad: Propiedad que referencia a la exactitud y totalidad de la información, mecanismos de procesamiento de datos, además de las modificaciones realizadas se encuentren debidamente auditadas y autorizadas.

Política de seguridad: Conjunto de lineamientos, guías, normas o buenas prácticas formalmente declaradas, de cumplimiento obligatorio por todos o cierto grupo de personas, con el objetivo de reducir la posibilidad de ocurrencia de eventos de vulnerabilidad y/o garantizar la ejecución de tareas establecidas.

Responsabilidades Generales

Comité de Seguridad: Responde ante el Fiscal General por la existencia y cumplimiento de las medidas dispuesta y orientadas para mantener un alto nivel de seguridad de la información, en relación a las necesidades de servicios y recursos disponibles.

El comité estará compuesto por:

- Coordinadores
- Directores de áreas misionales y habilitantes
- Encargado de seguridad de la Información

Encargado de Seguridad: Representante del Fiscal General en la definición, aplicación y monitoreo de los criterios de seguridad de la información. Para cumplir con este objetivo es necesario:

- Identificar y validar los activos de seguridad de la información a través de los propietarios, con validaciones periódicas.
- Analizar de forma permanente los niveles de riesgo, proponiendo a las autoridades ejecutivas las acciones o soluciones efectivas.
- Coordinar la implementación de las medidas aprobadas de forma oportuna.
- Difundir las políticas de seguridad al personal y a terceras partes.

Funcionarios: Personal que tiene la responsabilidad de cumplir con las medidas establecidas en este documento a nivel de su entorno laboral y fuera de este, además de tener la obligación de alertar de manera oportuna y a través de los canales y procedimientos establecidos cualquier situación que pueda poner en riesgo la seguridad de los activos de información.

Propietario de la información: Persona, personas o unidad adminitrativa responsable de la información y los procedimientos que la manipula, sean estos manuales, mecánicos o electrónicos, identificándolos claramente y definiendo su valor de manera que sea posible definir los controles apropiados para protegerlas.

Custodios de la información: Persona que tiene a cargo la responsabilidad de cuidar la información de cual no es propietario. Es el encargado de aplicar las medidas oportunas de seguridad de la información que se hayan definidos de acuerdo al valor del activo de la información, a esta categoría pertenecen:

- Personal de Tecnologías de la información son los responsables de crear, procesar o modificar la información de la institución y de los usuarios externos
- Personal que tiene acceso a toda o parte de la información de la institución, además de los usuarios externos

Adhesión a la Política

1. La presente política y las buenas prácticas, guías y normativa derivada o asociada a esta es de cumplimiento obligatorio de todo el personal de la institución.
2. El encargado de la seguridad de la información debe permanentemente el cumplimiento de las políticas, reportando los resultados obtenidos, trimestralmente durante el proceso de implementación de nuevos componentes o actualizaciones y semestralmente de los controles que no han sido modificados.
3. La Directiva de la Fiscalía General del Estado presentarán la petición para revocar o conceder a los usuarios privilegios para el acceso a la información y a las tecnologías que los soportan al Comité de seguridad de la información.
4. La Directiva de la Fiscalía General del Estado se reserva el derecho de presentar ante el Comité de Seguridad de la Información las sanciones disciplinarias en contra del personal que incumpla las normas expuestas

5. La Directivade la Fiscalía General del Estado realizará revisiones anuales de los contenidos de las políticas de seguridad para garantizar su vigencia y operatividad.

Protección de la Información

- La directiva de la Fiscalía General del Estado, acepta y reconoce que la seguridad de la información es un objetivo estratégico para la institución que debe ser apoyado y potencializado por todos los miembros que conforman la institución.

- Acuerda además que la información es un activo de alto valor y que debe ser protegido adecuadamente y en concordancia con los objetivos de la institución, requerimientos legales, administrativos y contractuales que sean necesarios y aplicables.

- Se tiene presente que no es posible eliminar totalmente el riesgo en ningún proceso, sin embargo es posible gestionar los incidentes de seguridad mediante las medidas definidas para proteger los activos de información. Estos deben ser analizados y aplicados en función de un análisis entre costo y beneficio para que sean aplicados oportunamente.

- Se deben realizar controles o análisis periódicos para definir controles adecuados a los posibles cambios en los activos de información.

Apoyo Dirección Ejecutiva

La directiva de la Fiscalía General del Estado destinará los recursos necesarios para una permanente capacitación y entrenamiento al personal de seguridad de la información en relación a la función que realice en esta tarea.

La directiva de la Fiscalía General del Estado destinará los recursos necesarios para una correcta gestión de la Seguridad de la Información.

De acuerdo a la gravedad de los riesgos que se puedan identificar estos se gestionarán para reducir a un nivel aceptable, considerando que los riesgos pueden ser aceptados, eludidos, transferidos o mitigados.

Para aquellos riesgos identificados y clasificados fuera de la categoría de aceptables, estos serán considerados para adoptar un conjunto de medidas apropias a fin de gestionarlos, además de disponer de los argumentos para indicar que:

- Las medidas adoptadas son suficientes para gestionar el nivel de riesgo y reducirlo a un nivel apropiado
- Las medidas tienen el costo apropiado para el beneficio que aportan a la solución o prevención de un incidente
- Las medidas reciben los recursos necesarios para su implementación.

Clasificación de la Información

- Cada propietario de la información debe realizar una clasificación de la información que se encuentra bajo su responsabilidad en términos de la importancia para la institución:
    - Confidencial
    - Uso Interno
    - Público

- Toda la información que no ha sido clasificada de alguna forma se considerará como de “Uso Interno” y recibirá los niveles de protección adecuados para esta categoría.

- El o los encargados de la seguridad de la información, deberán verificar que la clasificación utilizada para la información es la idónea y que los niveles de seguridad aplicados son los adecuados.

- Establecer para cada nivel de clasificación las medidas de protección correspondiente, además de indicar la obligatoriedad del cumplimiento de estas por parte del personal.

Uso de Activos de Información

1. Todos los activos de información serán utilizados exclusivamente para el proceder general e interinstitucional de la Fiscalía General del Estado, en concordancia con las políticas, estándares y procedimientos definidos para este efecto.

2. La Fiscalía General del Estado no permite el uso para fines personales de los activos de información

3. Los usuarios que utilizan los activos de información, tienen la obligación de cumplir:

    - La no divulgación de la información de la Fiscalía General del Estado clasificada como Confidencial o de Uso Interno, con la excepción indicada formalmente por el propietario de la información a quien se transfiere la responsabilidad de esta divulgación.

    - La prohibición de sacar información de las dependencias de la organización a menos de que hayan sido autorizados

    - La solicitud por escrito a cada propietario de la información, cuando sea necesario proporcionar a terceros información clasificada como confidencial o de Uso Interno, en concordancia con los controles específicos que se hayan definido.

    - El cumplimiento de los requisitos legales, normativos, administrativos y de presentarse el caso, contractuales relativos a la utilización de los activos de

información, incluyendo las políticas generales y particulares de seguridad de la información, que guardarán concordancia con las leyes vigentes.

- La protección de los elementos relativos al control de acceso, como por ejemplo contraseñas, dispositivos entregados, firma electrónica, entre otros, debido a que ser de uso individual estos son intransferibles y de responsabilidad de cada funcionario.
- La notificación oportuna de los incidentes que puedan poner en riesgo la seguridad de la información para adoptar las medidas necesarias.

Normas que componen la Política

Como parte de esta política, se establecen los dominios presentes en la norma ISO/IEC 27001, los cuales abarcan los activos de información que se desea proteger, estos son:

1. Norma de Funciones, Responsabilidades y Organización de Seguridad de la Información.
2. Norma de Gestión de Activos.
3. Norma de Seguridad de Recursos Humanos.
4. Norma de Seguridad Física y Ambiental.
5. Norma de Gestión de las Comunicaciones y Operaciones.
6. Norma de Gestión de Acceso.
7. Norma de Gestión de Incidentes de Seguridad de la Información.
8. Norma de Adquisición, Desarrollo y Mantenimiento de Seguridad de la Información.
9. Norma de Gestión de Continuidad del Negocio.
10. Norma de Cumplimiento.
11. Política de Seguridad de la Información.

Dr. Galo Chiriboga Zambrano

Fiscal General del Estado

Quito, 24 de Abril de 2013

3.2 Análisis de resultados

De acuerdo con la tabla Nro. 5, se indican cierta cantidad de incidentes en distintos niveles de vulnerabilidad, para este efecto necesitamos establecer mediante una metodología cuales son los posibles tratamientos a nivel general para cada uno de los niveles de vulnerabilidad. En este caso, de acuerdo con la metodología OCTAVE se establece un procedimiento de análisis, identificación y valoración de riesgos, para posteriormente iniciar el proceso para aplicar los respectivos enfoques de mitigación de riesgos.

Para este fin, primero definimos una matriz de riesgo relativo, de donde se pueden establecer rangos de acción y probabilidades, que posteriormente pueden ser cotejadas con una matriz de enfoque de riesgo.

En este caso, las valoraciones y probabilidades se presentan de esta forma:

	MATRIZ DE RIESGO RELATIVO				
PROBABILIDAD	**VALORACIÓN DE RIESGO**				
	41 - 60	**31 - 40**	**11 - 30**	**6 -10**	**0 – 5**
ALTO	RANGO 1	RANGO 1	RANGO 2	RANGO 2	RANGO 3
MEDIO	RANGO 1	RANGO 2	RANGO 2	RANGO 3	RANGO 4
BAJO	RANGO 2	RANGO 2	RANGO 3	RANGO 4	RANGO 4

Tabla Nro.10:Tabla de Matriz de Riesgo Relativo según metodología OCTAVE. Autor: Elaborado por el autor mediante metodología OCTAVE[26]

La matriz de enfoque de riesgo:

RANGO	ENFOQUE DE MITIGACIÓN
RANGO 1	TRANSFERIR
RANGO 2	MITIGAR
RANGO 3	APLAZAR
RANGO 4	ACEPTAR

Tabla Nro. 11: Acciones relacionadas con el riesgo a asumirse. Autor: Elaborado por el autor mediante metodología OCTAVE[27]

[26] Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson - Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process – Internet: http://www.cert.org/octave/allegro.html – Acceso: 23-04-2013

[27] Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson - Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process – Internet: http://www.cert.org/octave/allegro.html – Acceso: 23-04-2013

DENTIFICADOR	DECLARACIÓN DE RIESGO CONDICIÓN	PROBABILIDAD	VULNERABILIDAD	RANGO	ENFOQUE DE MITIGACIÓN
1	Contratación de enlaces sin redundancia y fallas del proveedor	ALTA	30	RANGO 1	TRANSFERIR
2	Topología en estrella y fallas en el nodo central de red	ALTA	60	RANGO 1	TRANSFERIR
3	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	ALTA	30	RANGO 1	TRANSFERIR
4	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	MEDIA	20	RANGO 2	MITIGAR
5	Falta de personal en los distintos puntos de atención de la FGE	ALTO	40	RANGO 1	TRANSFERIR
6	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	BAJA	20	RANGO 3	APLAZAR
7	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	ALTO	60	RANGO 1	TRANSFERIR
8	Equipamiento, infraestructura y recursos insuficientes	BAJA	10	RANGO 4	ACEPTAR
9	Equipamiento obsoleto o inexistente en los puntos de atención	MEDIA	40	RANGO 2	MITIGAR
10	Equipamiento insuficiente y de distintas generaciones	ALTA	60	RANGO 1	TRANSFERIR
11	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	ALTA	30	RANGO 1	TRANSFERIR

12	Información para el control y monitoreo de actividades del usuario imprecisa	ALTA	15	RANGO 2	MITIGAR
13	Catálogo de equipos manejado manualmente	MEDIA	20	RANGO 2	MITIGAR
14	Cronograma de respaldos inapropiado o con errores	MEDIA	40	RANGO 2	MITIGAR
15	Aplicativos con fallas o sin procesos de validación apropiados	MEDIA	40	RANGO 2	MITIGAR
16	Aplicativos o actividades no automatizadas	ALTA	30	RANGO 1	TRANSFERIR
17	Falta de capacitación a los usuarios en los aplicativos misionales	BAJA	10	RANGO 4	ACEPTAR
18	Información y manuales insuficientes	MEDIA	20	RANGO 2	MITIGAR
19	Distintos responsables para esas áreas	ALTA	30	RANGO 1	TRANSFERIR
20	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	MEDIA	40	RANGO 2	MITIGAR
21	Muchas variables necesarias para registrar las actividades de los fiscales	MEDIA	40	RANGO 2	MITIGAR
22	Metodologías de interpretación estadísticas dispares o incorrectas	ALTA	60	RANGO 1	TRANSFERIR

Resumen de enfoque de mitigación

CANTIDAD DE VULNERABILIDADES	ENFOQUE DE MITIGACION
10	TRANSFERIR
9	MITIGAR
1	APLAZAR
2	ACEPTAR

3.3Informe Técnico la situación propuesta

APLICACIÓN DE LA NORMA ISO 27001 PARA LA IMPLEMENTACIÓN DE UN SGSI EN LA FISCALÍA GENERAL DEL ESTADO

Elaborado por

Iván Narváez B.

Fecha de presentación: 25/04/2013

Índice

Tabla de contenidos

Tabla de contenidos

Introducción

El presente Informe Técnico, explica la situación actual de la FGE en términos relacionados con la Seguridad de la Información.

Los temas presentados en este informe, responden a los procesos críticos que engloba el giro del negocio de la institución, afianzándose en asuntos de confidencialidad, disponibilidad e integridad de losactivos de información.

Para abordar estos temas, se plantea un análisis y evaluación de riesgos mediante metodologías técnicas y la aplicación de la norma ISO/IEC 27001 relacionada con Seguridad de la Información.

Antecedentes

Centrándose en el área de gestión de la Fiscalía General del Estado, está institución mantiene una gran cantidad de información, mayormente en medios impresos, debido a las investigaciones que realizan los fiscales son sustentadas en documentos físicos, según la interpretación de normativa vigente, durante varias decenas de años. Así también cuenta con un conjunto igualmente grande de documentos de orden administrativo, siendo las direcciones de Recursos Humanos, Administrativo Financiero las que mayor cantidad de documentación archivan en las distintas zonas destinadas a este fin.

Esta información se recolecta desde varios puntos donde es receptada, procesada y almacenada para que se pueda utilizar por sus empleados y directivos con fines de trabajo (enriquecimiento de valor) y gerenciamiento (para la toma de decisiones) y esta puede ser transmitida por medios telemáticos dentro y fuera de las instalaciones de la empresa o institución.

Además, el valor de la información está en directa proporción por el uso que se pueda dar, sea esta por el generador o dueño de la información, que generalmente son los procesos relacionados con las Direcciones Administrativas, así como por el uso autorizado o no, de esta por otra persona o empresa. Han sido varios los casos que se han denunciado acerca de organismos del sector público que han establecido políticas de seguridad inadecuadas en sus registros electrónicos posibilitando que terceros se apropien de la información custodiada y la puedan comercializar dentro y fuera del país con fines ilícitos.

Siendo el concepto de Información el eje central de donde parte la necesidad de la aplicación de una norma y un sistema de gestión en una institución pública o privada, se define como información a cualquier conjunto de datos que se encuentren organizados, que representan valor a la organización o institución a la que pertenecen, independientemente que estos se encuentren almacenados o transmitidos en forma escrita, gráfica, oral, en correo electrónico, en bases de datos, fax, formato de audio, etc.

Alcance

El alcance de este informe es el delimitado por las actividades misionales y administrativas de la FGE en su proceder actual presentes en la RESOLUCIÓN N° 03-A-FGE-2012 (Estatuto Orgánico por procesos) particularizados en los procedimientos que agregan de valor a los productos que la institución desarrolla, en contraste con la normativa ISO/IEC 27001 (Tecnología de la Información – Sistemas de Gestión de seguridad de la información - Requerimientos), primera edición de 2005-10-15.

Las valoraciones de riesgos se realizan mediante la metodología COSO y en enfoque de riesgos referencia a la metodología OCTAVE.

Objetivo General

Presentar a la Directiva de la FGE un análisis técnico relacionado con los procedimientos de Seguridad de Información en la institución, en miras de implementar un Sistema de Gestión de Seguridad de la Información.

Observar los riesgos presentes en seguridad de la información a fin de demostrar que la adopción de una SGSI es una decisión estratégica para la institución, que mejorará la credibilidad frente a la ciudadanía, mejorará y transparentará procesos.

Objetivo Específico

Analizar los procesos estratégicos desde un punto de vista de riesgo a la gestión para entender los requerimientos de seguridad mínimos para un funcionamiento óptimo.

Evaluar la situación actual en termas de Seguridad de la Información para determinar los niveles de vulnerabilidad en este tema.

Observar de manera breve los controles necesarios para el manejo de riesgos desde un enfoque relacionado con la norma ISO/IEC 27001.

Definir una política de seguridad inicial para iniciar el proceso de certificación de la norma ISO/IEC 27001.

Realizar un esquema de enfoque de riesgos para las vulnerabilidades identificadas.

Desarrollo/Hallazgos/Resultados

Análisis de la situación actual

En función del riesgo o vulnerabilidad en la Seguridad de la Información, se presenta el siguiente cuadro que describe de forma cualitativa las vulnerabilidades encontradas en el actual modelo de gestión de la FGE.

Matriz de Riesgos

ID	RIESGO	DECLARACIÓN DE RIESGO		NIVEL DE VULNERABILIDAD
		CONDICIÓN	CONSECUENCIA	
1	Interrupciones en comunicaciones	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país	IMPORTANTE
2	Topología de red incorrecta	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional	INACEPTABLE
3	Mal dimensionamiento de las necesidades institucionales	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	Servicio lento y deficiente.	IMPORTANTE
			Poco control sobre las actividades que se realizan en esos puntos.	
			Se asocia a un mal servicio en general de toda la institución	

4	Capacitación del personal	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión	MODERADO
5	Disponibilidad de Recurso humano	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional	IMPORTANTE
6	Áreas Físicas para Data Center	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	Interrupción del servicio y daño físico en el equipamiento de servidores y equipos de comunicación.	MODERADO
7	Conexión a internet	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	Los sistemas misionales de la FGE se encuentran desarrollados para que sean accedidos por internet, por lo que al disponer de un servicio itinerante dificulta el ofrecimiento de servicios a los usuarios	INACEPTABLE

8	Central Telefónica	Equipamiento, infraestructura y recursos insuficientes	La comunicación telefónica es inexistente en algunos lugares, los servicios no son centralizados, dificultando las actividades de gestión de los funcionarios en puntos remotos del país.	TOLERABLE
9	Equipos de cómputo para usuarios internos	Equipamiento obsoleto o inexistente en los puntos de atención	Descontento por la inequidad en la atención de los requerimientos de los usuarios internos	IMPORTANTE
			Lentitud en los procesos de atención al usuario	
			Manejo discrecional de los procesos oficiales para atención al público y fiscalía especializada.	

10	Equipamiento de servidores para uso institucional	Equipamiento insuficiente y de distintas generaciones	Sistemas no funcionan de manera óptima, con bajo nivel de procesamiento, sumado a un creciente número de instituciones que consumen información de la FGE en decremento del nivel de satisfacción sobre el uso de las herramientas informáticas para los usuarios internos y externos,	INACEPTABLE
11	HelpDesk	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	Falta de retroalimentación para procedimientos de mejora	IMPORTANTE
			Discrecionalidad o inatención a las demandas del usuario	
			Retraso en la atención del usuario externo	
			Falta de métricas de rendimiento por analista a cargo de las distintas áreas de soporte al usuario	

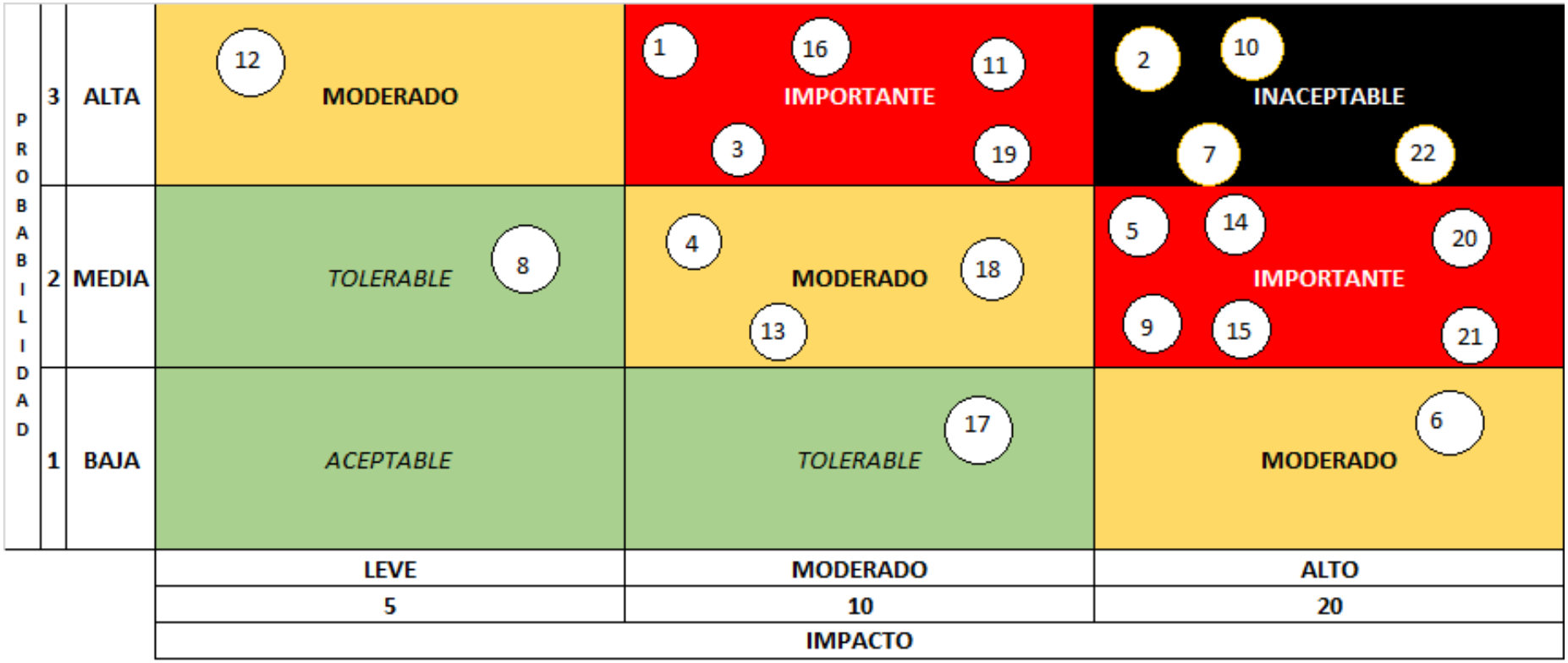
12	Información de usuarios internos	Información para el control y monitoreo de actividades del usuario imprecisa	Perfiles y acceso de usuario inadecuados para recursos sensibles.	MODERADO
			Información desactualizada e incompleta	
13	Catálogo de equipos	Catálogo de equipos manejado manualmente	Información imprecisa y desactualizada de catálogos es remitida periódicamente por los analistas provinciales en hojas electrónicas para que sea condensada en Quito	MODERADO
14	Respaldos de Base de Datos	Cronograma de respaldos inapropiado o con errores	Procedimientos de auditoría incompletos	IMPORTANTE
			En caso de fallos críticos no se puede recuperar toda la información ingresada por los usuarios internos	
			Impacto social debido a la sensibilidad de la información	

15	Aplicativos	Aplicativos con fallas o sin procesos de validación apropiados	Errores en el procesamiento o errores que imposibilitan el uso regular de los servicios de la institución	IMPORTANTE
16		Aplicativos o actividades no automatizadas	Información registrada manualmente y sin control sobre esos procedimientos	IMPORTANTE
17		Falta de capacitación a los usuarios en los aplicativos misionales	Usuarios no utilizan los aplicativos de forma apropiada generando errores en las estadísticas de atención al usuario	TOLERABLE
18	Varios sistemas de documentación	Información y manuales insuficientes	Sistemas poco difundidos y usados discrecionalmente	MODERADO
19		Distintos responsables para esas áreas	No existe un responsable claro para dar soporte a los usuarios y encargado de	IMPORTANTE

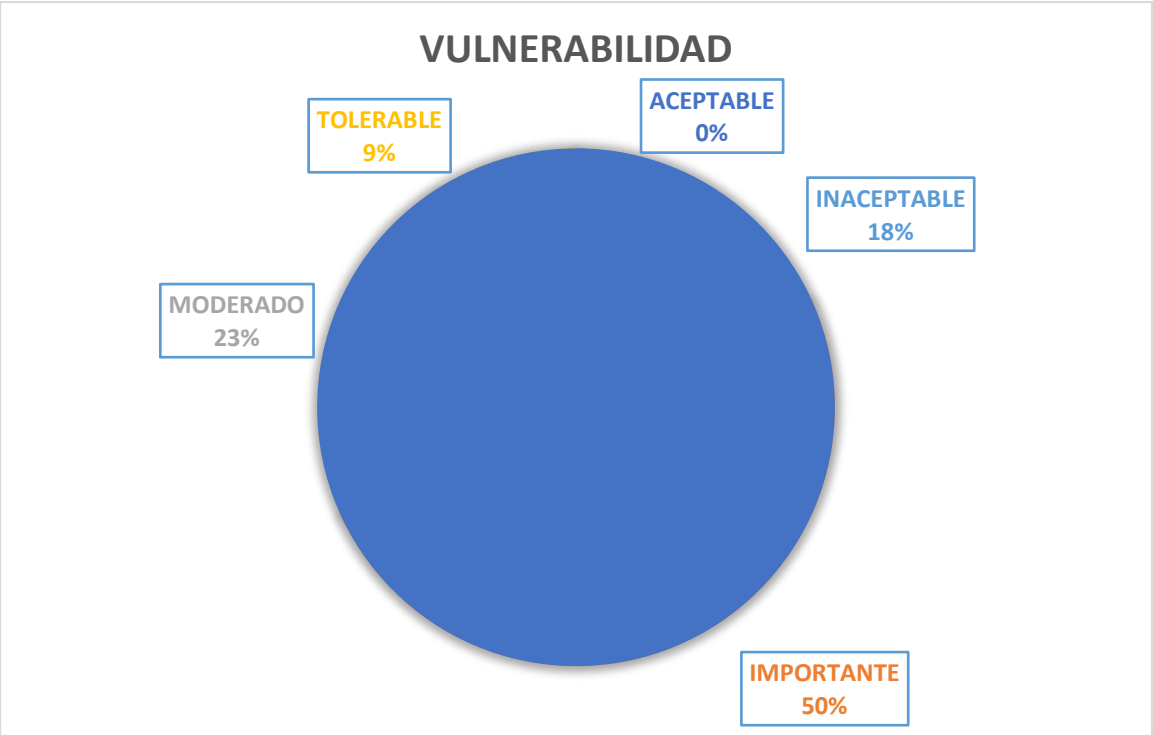
			gestionar la capacitación y garantías.	
20	Sistemas de archivos manuales o inexistentes	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	Dificultad para acceder a la información de los expediente ingresados al Archivo central	IMPORTANTE
21	Personal insuficiente	Muchas variables necesarias para registrar las actividades de los fiscales	Lentitud en el proceso de registro de los expedientes que se van a ingresar a los distintos archivos.	IMPORTANTE
22	Estadísticas incoherentes	Metodologías de interpretación estadísticas dispares o incorrectas	Análisis criminológico inexacto	INACEPTABLE
			Pérdida de credibilidad en las instituciones del sector justicia	
			Mala percepción del trabajo de los funcionarios judiciales	

Mapa de Riesgos

En la medida de poder representar los resultados obtenidos se expone el siguiente Mapa de Riesgos, que muestra las zonas de vulnerabilidad presentes que deben ser gestionadas.



Evaluación de riesgos – Reporte



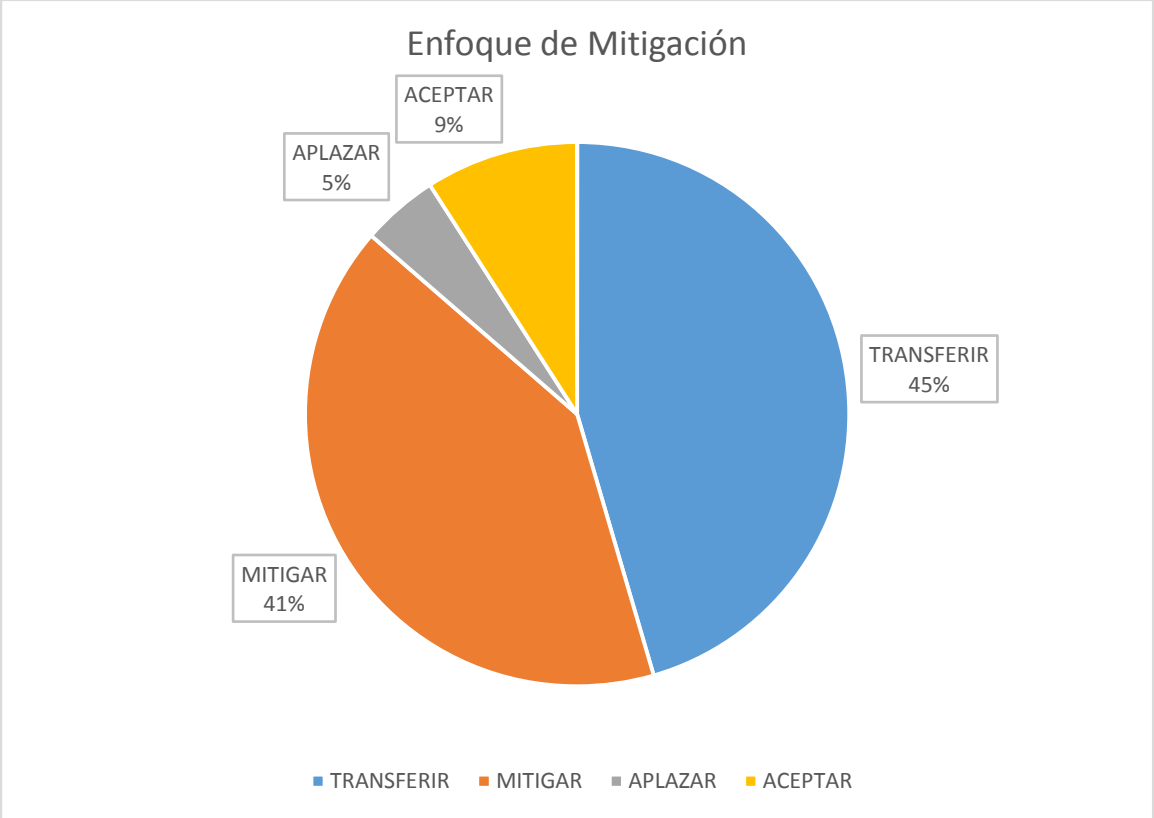
VALORACIÓN	CANTIDAD DE RIESGOS IDENTIFICADOS
INACEPTABLE	4
IMPORTANTE	11
MODERADO	5
TOLERABLE	2
ACEPTABLE	0
TOTAL	22

Enfoque de Riesgo - Reporte

DENTIFICADOR	DECLARACIÓN DE RIESGO CONDICIÓN	PROBABILIDAD	VULNERABILIDAD	RANGO	ENFOQUE DE MITIGACIÓN
1	Contratación de enlaces sin redundancia y fallas del proveedor	ALTA	30	RANGO 1	TRANSFERIR
2	Topología en estrella y fallas en el nodo central de red	ALTA	60	RANGO 1	TRANSFERIR
3	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	ALTA	30	RANGO 1	TRANSFERIR
4	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	MEDIA	20	RANGO 2	MITIGAR
5	Falta de personal en los distintos puntos de atención de la FGE	ALTO	40	RANGO 1	TRANSFERIR
6	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	BAJA	20	RANGO 3	APLAZAR
7	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	ALTO	60	RANGO 1	TRANSFERIR
8	Equipamiento, infraestructura y recursos insuficientes	BAJA	10	RANGO 4	ACEPTAR
9	Equipamiento obsoleto o inexistente en los puntos de atención	MEDIA	40	RANGO 2	MITIGAR
10	Equipamiento insuficiente y de distintas generaciones	ALTA	60	RANGO 1	TRANSFERIR
11	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	ALTA	30	RANGO 1	TRANSFERIR

12	Información para el control y monitoreo de actividades del usuario imprecisa	ALTA	15	RANGO 2	MITIGAR
13	Catálogo de equipos manejado manualmente	MEDIA	20	RANGO 2	MITIGAR
14	Cronograma de respaldos inapropiado o con errores	MEDIA	40	RANGO 2	MITIGAR
15	Aplicativos con fallas o sin procesos de validación apropiados	MEDIA	40	RANGO 2	MITIGAR
16	Aplicativos o actividades no automatizadas	ALTA	30	RANGO 1	TRANSFERIR
17	Falta de capacitación a los usuarios en los aplicativos misionales	BAJA	10	RANGO 4	ACEPTAR
18	Información y manuales insuficientes	MEDIA	20	RANGO 2	MITIGAR
19	Distintos responsables para esas áreas	ALTA	30	RANGO 1	TRANSFERIR
20	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	MEDIA	40	RANGO 2	MITIGAR
21	Muchas variables necesarias para registrar las actividades de los fiscales	MEDIA	40	RANGO 2	MITIGAR
22	Metodologías de interpretación estadísticas dispares o incorrectas	ALTA	60	RANGO 1	TRANSFERIR

Resumen de enfoque de mitigación



CANTIDAD DE VULNERABILIDADES	ENFOQUE DE MITIGACION
10	TRANSFERIR
9	MITIGAR
1	APLAZAR
2	ACEPTAR

Conclusiones

Del análisis realizado se pueden indicar las siguientes conclusiones:

- Mediante metodologías de evaluación de riesgos es factible realizar un análisis de la situación actual de cualquier organización, en este caso se usaron COSO y OCTAVE si embargo existen otros procedimientos como la ISO/IEC 27005 o ISO/IEC 13335.

- Analizando las características de la institución que se ha sometido a estudio, se revela la necesidad de implementar un SGSI, debido a la complejidad de los procesos, normativa legal vigente y cantidad de registros que se ingresan y analizan cada día.

- No se encuentra presente en la cadena de valor institucional los procesos relacionados con seguridad de la información, aun cuando este es el activo más valioso de la institución.

- No se cuenta con el Comité de Seguridad de la información en la institución.

- La normativa del sector público ni la normativa administrativa interna no contempla planes claros relacionados con la seguridad de la información.

- Existen problemas graves en el manejo de seguridad de la información. El 18% de los riesgos identificados se evaluaron como INACEPTABLES, la mitad de los riesgos se evalúan como IMPORTANTES, alrededor de la cuarta parte de estos se identifican como de riesgo MODERADO y 9% como TOLERABLE.

- No está presente el concepto de SGSI en la FGE, por cuanto recae en varios componentes las variables que inducen vulnerabilidad, iniciando por una falta de cultura de seguridad de información entre los empleados hasta la implementación de controles formales en el mismo tema.

- El enfoque de TRANSFERIR el riesgo es la actividad que con mayor frecuencia se presenta, alrededor del 45% de las vulnerabilidades demandan esta acción; La MITIGACION del riesgo es la segunda forma de enfoque referida con el 41%, las

formas de APLAZAMIENTO Y ACEPTACIÓN del riesgo aportan el 5% y 9% de los enfoques posibles para el problema de seguridad de la información.

- No se dispone de análisis anteriores a evaluaciones de seguridad de la Información.
- No se dispone de un responsable de seguridad de la información, que pueda establecer nuevas políticas para posteriores análisis y monitorear el avance en el proceso de implementación.

Recomendaciones

Se pueden hacer las recomendaciones relacionadas con el SGSI que se desea aplicar:

- Establecer formalmente en la institución un Comité de Seguridad de la Información, debido a que este es el responsable de aprobar y gestionar varios componentes fundamentales del SGSI.
- Se debe nombrar un Responsable de la Seguridad de la Información para que asuma el rol ejecutivo en las actividades relacionadas con la seguridad de los activos de información.
- Se debe promover de manera más agresiva los procedimientos relacionados con seguridad de la información en todas las unidades administrativas y misionales de la FGE a fin de iniciar un proceso de certificación con menor impacto hacia los usuarios.
- Se deben iniciar los procesos contractuales o los necesarios para aplicar la TRANSFERENCIA de riesgo a terceros de acuerdo a la naturaleza del caso, estos pueden ser a través de aseguradoras.
- Para el caso de MITIGACIÓN de riesgos es necesario establecer los controles necesarios para implementarlos lo más pronto posible, sea el caso de controles disuasivos o compensatorios de acuerdo al caso que sea necesario.
- En el caso de los APLAZAMIENTO de riegos, se deben establecer planes y cronogramas para solucionar los potenciales problemas que pueden ocasionar.

- En el caso de ACEPTACION de riesgos, documentar las características de estas vulnerabilidades para establecer un procedimiento para que cuando sea posible mediante inversión económica o nueva tecnología este pueda ser mitigado o gestionado.

3.4 Informe Ejecutivo de la situación propuesta

APLICACIÓN DE LA NORMA ISO 27001 PARA LA IMPLEMENTACIÓN DE UN SGSI EN LA FISCALÍA GENERAL DEL ESTADO

Elaborado por

Iván Narváez B.

Fecha de presentación: 25/04/2013

Índice

Tabla de contenidos

Introducción

El presente Informe Técnico, explica la situación actual de la FGE en términos relacionados con la Seguridad de la Información.

Los temas presentados en este informe, responden a los procesos críticos que engloba el giro del negocio de la institución, afianzándose en asuntos de confidencialidad, disponibilidad e integridad de losactivos de información.

Para abordar estos temas, se plantea un análisis y evaluación de riesgos mediante metodologías técnicas y la aplicación de la norma ISO/IEC 27001 relacionada con Seguridad de la Información.

Antecedentes

Centrándose en el área de gestión de la Fiscalía General del Estado, está institución mantiene una gran cantidad de información, mayormente en medios impresos, debido a las investigaciones que realizan los fiscales son sustentadas en documentos físicos, según la interpretación de normativa vigente, durante varias decenas de años. Así también cuenta con un conjunto igualmente grande de documentos de orden administrativo, siendo las direcciones de Recursos Humanos, Administrativo Financiero las que mayor cantidad de documentación archivan en las distintas zonas destinadas a este fin.

Esta información se recolecta desde varios puntos donde es receptada, procesada y almacenada para que se pueda utilizar por sus empleados y directivos con fines de trabajo (enriquecimiento de valor) y gerenciamiento (para la toma de decisiones) y esta puede ser transmitida por medios telemáticos dentro y fuera de las instalaciones de la empresa o institución.

Además, el valor de la información está en directa proporción por el uso que se pueda dar, sea esta por el generador o dueño de la información, que generalmente son los procesos relacionados con las Direcciones Administrativas, así como por el uso autorizado o no, de esta por otra persona o empresa. Han sido varios los casos que se

han denunciado acerca de organismos del sector público que han establecido políticas de seguridad inadecuadas en sus registros electrónicos posibilitando que terceros se apropien de la información custodiada y la puedan comercializar dentro y fuera del país con fines ilícitos.

Siendo el concepto de Información el eje central de donde parte la necesidad de la aplicación de una norma y un sistema de gestión en una institución pública o privada, se define como información a cualquier conjunto de datos que se encuentren organizados, que representan valor a la organización o institución a la que pertenecen, independientemente que estos se encuentren almacenados o transmitidos en forma escrita, gráfica, oral, en correo electrónico, en bases de datos, fax, formato de audio, etc.

Alcance

El alcance de este informe es el delimitado por las actividades misionales y administrativas de la FGE en su proceder actual presentes en la RESOLUCIÓN N° 03-A-FGE-2012 (Estatuto Orgánico por procesos) particularizados en los procedimientos que agregan de valor a los productos que la institución desarrolla, en contraste con la normativa ISO/IEC 27001 (Tecnología de la Información – Sistemas de Gestión de seguridad de la información - Requerimientos), primera edición de 2005-10-15.

Las valoraciones de riesgos se realizan mediante la metodología COSO y en enfoque de riesgos referencia a la metodología OCTAVE.

Objetivo General

Presentar a la Directiva de la FGE un análisis técnico relacionado con los procedimientos de Seguridad de Información en la institución, en miras de implementar un Sistema de Gestión de Seguridad de la Información.

Observar los riesgos presentes en seguridad de la información a fin de demostrar que la adopción de una SGSI es una decisión estratégica para la institución, que mejorará la credibilidad frente a la ciudadanía, mejorará y transparentará procesos.

Objetivo Específico

Analizar los procesos estratégicos desde un punto de vista de riesgo a la gestión para entender los requerimientos de seguridad mínimos para un funcionamiento óptimo.

Evaluar la situación actual en termas de Seguridad de la Información para determinar los niveles de vulnerabilidad en este tema.

Observar de manera breve los controles necesarios para el manejo de riesgos desde un enfoque relacionado con la norma ISO/IEC 27001.

Definir una política de seguridad inicial para iniciar el proceso de certificación de la norma ISO/IEC 27001.

Realizar un esquema de enfoque de riesgos para las vulnerabilidades identificadas.

Desarrollo/Hallazgos/Resultados

Análisis de la situación actual

En función del riesgo o vulnerabilidad en la Seguridad de la Información, se presenta el siguiente cuadro que describe de forma cualitativa las vulnerabilidades encontradas en el actual modelo de gestión de la FGE.

Matriz de Riesgos

ID	RIESGO	DECLARACIÓN DE RIESGO		NIVEL DE VULNERABILIDAD
		CONDICIÓN	CONSECUENCIA	
1	Interrupciones en comunicaciones	Contratación de enlaces sin redundancia y fallas del proveedor	Interrupción del servicio en atención al público y fiscalía especializada en varios puntos del país	IMPORTANTE
2	Topología de red incorrecta	Topología en estrella y fallas en el nodo central de red	Falla de todo el sistema interconectado a nivel nacional	INACEPTABLE
3	Mal dimensionamiento de las necesidades institucionales	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	Servicio lento y deficiente.	IMPORTANTE
			Poco control sobre las actividades que se realizan en esos puntos.	
			Se asocia a un mal servicio en general de toda la institución	

4	Capacitación del personal	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	Las inversiones en tecnología no son explotadas completamente, ni tampoco se puede observar los réditos de esa inversión	MODERADO
5	Disponibilidad de Recurso humano	Falta de personal en los distintos puntos de atención de la FGE	No se cuenta con personal suficiente para atender las necesidades de todos los usuarios a nivel nacional	IMPORTANTE
6	Áreas Físicas para Data Center	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	Interrupción del servicio y daño físico en el equipamiento de servidores y equipos de comunicación.	MODERADO
7	Conexión a internet	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	Los sistemas misionales de la FGE se encuentran desarrollados para que sean accedidos por internet, por lo que al disponer de un servicio itinerante dificulta el ofrecimiento de servicios a los usuarios	INACEPTABLE

8	Central Telefónica	Equipamiento, infraestructura y recursos insuficientes	La comunicación telefónica es inexistente en algunos lugares, los servicios no son centralizados, dificultando las actividades de gestión de los funcionarios en puntos remotos del país.	TOLERABLE
9	Equipos de cómputo para usuarios internos	Equipamiento obsoleto o inexistente en los puntos de atención	Descontento por la inequidad en la atención de los requerimientos de los usuarios internos	IMPORTANTE
			Lentitud en los procesos de atención al usuario	
			Manejo discrecional de los procesos oficiales para atención al público y fiscalía especializada.	

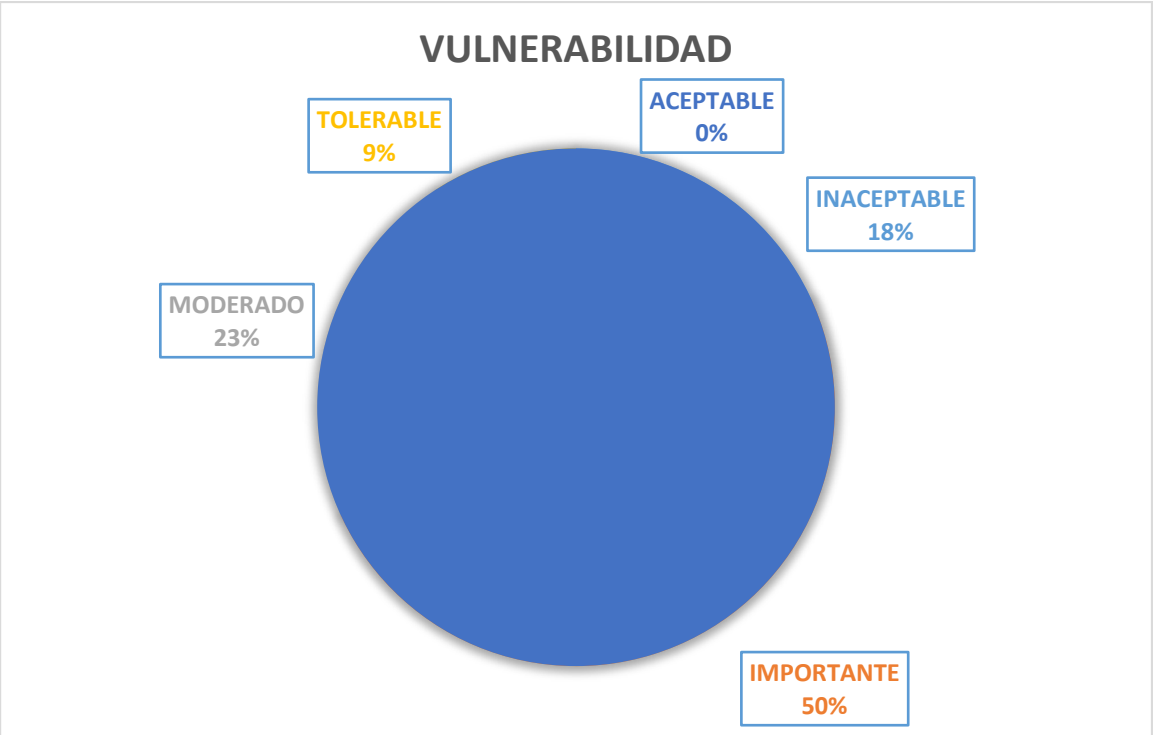
10	Equipamiento de servidores para uso institucional	Equipamiento insuficiente y de distintas generaciones	Sistemas no funcionan de manera óptima, con bajo nivel de procesamiento, sumado a un creciente número de instituciones que consumen información de la FGE en decremento del nivel de satisfacción sobre el uso de las herramientas informáticas para los usuarios internos y externos,	INACEPTABLE
11	HelpDesk	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	Falta de retroalimentación para procedimientos de mejora	IMPORTANTE
			Discrecionalidad o inatención a las demandas del usuario	
			Retraso en la atención del usuario externo	
			Falta de métricas de rendimiento por analista a cargo de las distintas áreas de soporte al usuario	

12	Información de usuarios internos	Información para el control y monitoreo de actividades del usuario imprecisa	Perfiles y acceso de usuario inadecuados para recursos sensibles.	MODERADO
			Información desactualizada e incompleta	
13	Catálogo de equipos	Catálogo de equipos manejado manualmente	Información imprecisa y desactualizada de catálogos es remitida periódicamente por los analistas provinciales en hojas electrónicas para que sea condensada en Quito	MODERADO
14	Respaldos de Base de Datos	Cronograma de respaldos inapropiado o con errores	Procedimientos de auditoría incompletos	IMPORTANTE
			En caso de fallos críticos no se puede recuperar toda la información ingresada por los usuarios internos	
			Impacto social debido a la sensibilidad de la información	

15	Aplicativos	Aplicativos con fallas o sin procesos de validación apropiados	Errores en el procesamiento o errores que imposibilitan el uso regular de los servicios de la institución	IMPORTANTE
16		Aplicativos o actividades no automatizadas	Información registrada manualmente y sin control sobre esos procedimientos	IMPORTANTE
17		Falta de capacitación a los usuarios en los aplicativos misionales	Usuarios no utilizan los aplicativos de forma apropiada generando errores en las estadísticas de atención al usuario	TOLERABLE
18	Varios sistemas de documentación	Información y manuales insuficientes	Sistemas poco difundidos y usados discrecionalmente	MODERADO
19		Distintos responsables para esas áreas	No existe un responsable claro para dar soporte a los usuarios y encargado de	IMPORTANTE

			gestionar la capacitación y garantías.	
20	Sistemas de archivos manuales o inexistentes	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	Dificultad para acceder a la información de los expediente ingresados al Archivo central	IMPORTANTE
21	Personal insuficiente	Muchas variables necesarias para registrar las actividades de los fiscales	Lentitud en el proceso de registro de los expedientes que se van a ingresar a los distintos archivos.	IMPORTANTE
22	Estadísticas incoherentes	Metodologías de interpretación estadísticas dispares o incorrectas	Análisis criminológico inexacto	INACEPTABLE
			Pérdida de credibilidad en las instituciones del sector justicia	
			Mala percepción del trabajo de los funcionarios judiciales	

Evaluación de riesgos – Reporte



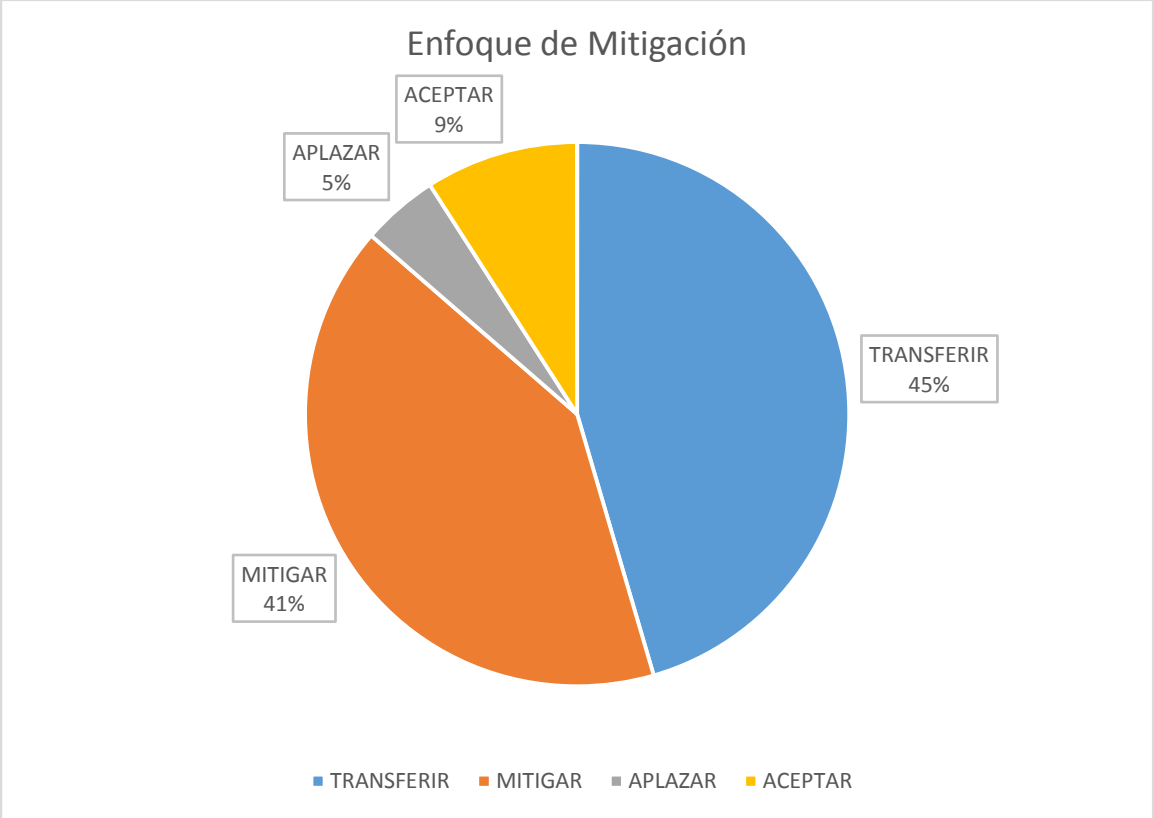
VALORACIÓN	CANTIDAD DE RIESGOS IDENTIFICADOS
INACEPTABLE	4
IMPORTANTE	11
MODERADO	5
TOLERABLE	2
ACEPTABLE	0
TOTAL	22

Enfoque de Riesgo - Reporte

DENTIFICADOR	DECLARACIÓN DE RIESGO CONDICIÓN	ENFOQUE DE MITIGACIÓN
1	Contratación de enlaces sin redundancia y fallas del proveedor	TRANSFERIR
2	Topología en estrella y fallas en el nodo central de red	TRANSFERIR
3	Sub-dimensionamiento de ancho de banda para conexión con los servidores internos e internet en los puntos de recepción fuera de la capital provincial	TRANSFERIR
4	Los nuevos equipos o servicios contratados no capacitan de forma óptima al personal técnico	MITIGAR
5	Falta de personal en los distintos puntos de atención de la FGE	TRANSFERIR
6	Áreas destinadas para este efecto sin la seguridad y equipamiento necesario.	APLAZAR
7	Extensa cobertura de la institución pero con servicios no óptimos ofrecidos por terceros	TRANSFERIR
8	Equipamiento, infraestructura y recursos insuficientes	ACEPTAR
9	Equipamiento obsoleto o inexistente en los puntos de atención	MITIGAR
10	Equipamiento insuficiente y de distintas generaciones	TRANSFERIR
11	Procedimientos no estandarizados, documentados y registro de cantidad de tickets resueltos por analista	TRANSFERIR

12	Información para el control y monitoreo de actividades del usuario imprecisa	MITIGAR
13	Catálogo de equipos manejado manualmente	MITIGAR
14	Cronograma de respaldos inapropiado o con errores	MITIGAR
15	Aplicativos con fallas o sin procesos de validación apropiados	MITIGAR
16	Aplicativos o actividades no automatizadas	TRANSFERIR
17	Falta de capacitación a los usuarios en los aplicativos misionales	ACEPTAR
18	Información y manuales insuficientes	MITIGAR
19	Distintos responsables para esas áreas	TRANSFERIR
20	Gran cantidad de información registrados en medios físicos que se ingresan al Archivo central	MITIGAR
21	Muchas variables necesarias para registrar las actividades de los fiscales	MITIGAR
22	Metodologías de interpretación estadísticas dispares o incorrectas	TRANSFERIR

Resumen de enfoque de mitigación



CANTIDAD DE VULNERABILIDADES	ENFOQUE DE MITIGACION
10	TRANSFERIR
9	MITIGAR
1	APLAZAR
2	ACEPTAR

Conclusiones

Del análisis realizado se pueden indicar las siguientes conclusiones:

- Analizando las características de la institución que se ha sometido a estudio, se revela la necesidad de implementar un SGSI, debido a la complejidad de los procesos, normativa legal vigente y cantidad de registros que se ingresan y analizan cada día.

- No se encuentra presente en la cadena de valor institucional los procesos relacionados con seguridad de la información, aun cuando este es el activo más valioso de la institución.

- No se cuenta con el Comité de Seguridad de la información en la institución.

- La normativa del sector público ni la normativa administrativa interna no contempla planes claros relacionados con la seguridad de la información.

- Existen problemas graves en el manejo de seguridad de la información. El 18% de los riesgos identificados se evaluaron como INACEPTABLES, la mitad de los riesgos se evalúan como IMPORTANTES, alrededor de la cuarta parte de estos se identifican como de riesgo MODERADO y 9% como TOLERABLE.

- No está presente el concepto de SGSI en la FGE, por cuanto recae en varios componentes las variables que inducen vulnerabilidad, iniciando por una falta de cultura de seguridad de información entre los empleados hasta la implementación de controles formales en el mismo tema.

- El enfoque de TRANSFERIR el riesgo es la actividad que con mayor frecuencia se presenta, alrededor del 45% de las vulnerabilidades demandan esta acción; La MITIGACION del riesgo es la segunda forma de enfoque referida con el 41%, las formas de APLAZAMIENTO Y ACEPTACIÓN del riesgo aportan el 5% y 9% de los enfoques posibles para el problema de seguridad de la información.

- No se dispone de un responsable de seguridad de la información, que pueda establecer nuevas políticas para posteriores análisis y monitorear el avance en el proceso de implementación.

Recomendaciones

Se pueden hacer las recomendaciones relacionadas con el SGSI que se desea aplicar:

- Establecer formalmente en la institución un Comité de Seguridad de la Información, debido a que este es el responsable de aprobar y gestionar varios componentes fundamentales del SGSI.

- Se debe nombrar un Responsable de la Seguridad de la Información para que asuma el rol ejecutivo en las actividades relacionadas con la seguridad de los activos de información.

- Se debe promover de manera más agresiva los procedimientos relacionados con seguridad de la información en todas las unidades administrativas y misionales de la FGE a fin de iniciar un proceso de certificación con menor impacto hacia los usuarios.

- Se deben iniciar los procesos contractuales o los necesarios para aplicar la TRANSFERENCIA de riesgo a terceros de acuerdo a la naturaleza del caso, estos pueden ser a través de aseguradoras.

- Para el caso de MITIGACIÓN de riesgos es necesario establecer los controles necesarios para implementarlos lo más pronto posible, sea el caso de controles disuasivos o compensatorios de acuerdo al caso que sea necesario.

- En el caso de los APLAZAMIENTO de riegos, se deben establecer planes y cronogramas para solucionar los potenciales problemas que pueden ocasionar.

- En el caso de ACEPTACION de riesgos, documentar las características de estas vulnerabilidades para establecer un procedimiento para que cuando sea posible mediante inversión económica o nueva tecnología este pueda ser mitigado o gestionado.

4. CAPÍTULO IV – CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Del análisis realizado se pueden indicar las siguientes conclusiones:

- Mediante metodologías de evaluación de riesgos es factible realizar un análisis de la situación actual de cualquier organización, en este caso se usaron COSO y OCTAVE si embargo existen otros procedimientos como la ISO/IEC 27005 o ISO/IEC 13335.

- Analizando las características de la institución que se ha sometido a estudio, se revela la necesidad de implementar un SGSI, debido a la complejidad de los procesos, normativa legal vigente y cantidad de registros que se ingresan y analizan cada día.

- No se encuentra presente en la cadena de valor institucional los procesos relacionados con seguridad de la información, aun cuando este es el activo más valioso de la institución.

- No se cuenta con el Comité de Seguridad de la información en la institución.

- La normativa del sector público ni la normativa administrativa interna no contempla planes claros relacionados con la seguridad de la información.

- Existen problemas graves en el manejo de seguridad de la información. El 18% de los riesgos identificados se evaluaron como INACEPTABLES, la mitad de los riesgos se evalúan como IMPORTANTES, alrededor de la cuarta parte de estos se identifican como de riesgo MODERADO y 9% como TOLERABLE.

- No está presente el concepto de SGSI en la FGE, por cuanto recae en varios componentes las variables que inducen vulnerabilidad, iniciando por una falta de cultura de seguridad de información entre los empleados hasta la implementación de controles formales en el mismo tema.

- El enfoque de TRANSFERIR el riesgo es la actividad que con mayor frecuencia se presenta, alrededor del 45% de las vulnerabilidades demandan esta acción; La MITIGACION del riesgo es la segunda forma de enfoque referida con el 41%, las

formas de APLAZAMIENTO Y ACEPTACIÓN del riesgo aportan el 5% y 9% de los enfoques posibles para el problema de seguridad de la información.

- No se dispone de análisis anteriores a evaluaciones de seguridad de la Información.
- No se dispone de un responsable de seguridad de la información, que pueda establecer nuevas políticas para posteriores análisis y monitorear el avance en el proceso de implementación.

4.2 Recomendaciones

Se pueden hacer las recomendaciones relacionadas con el SGSI que se desea aplicar:

- Establecer formalmente en la institución un Comité de Seguridad de la Información, debido a que este es el responsable de aprobar y gestionar varios componentes fundamentales del SGSI.
- Se debe nombrar un Responsable de la Seguridad de la Información para que asuma el rol ejecutivo en las actividades relacionadas con la seguridad de los activos de información.
- Se debe promover de manera más agresiva los procedimientos relacionados con seguridad de la información en todas las unidades administrativas y misionales de la FGE a fin de iniciar un proceso de certificación con menor impacto hacia los usuarios.
- Se deben iniciar los procesos contractuales o los necesarios para aplicar la TRANSFERENCIA de riesgo a terceros de acuerdo a la naturaleza del caso, estos pueden ser a través de aseguradoras.
- Para el caso de MITIGACIÓN de riesgos es necesario establecer los controles necesarios para implementarlos lo más pronto posible, sea el caso de controles disuasivos o compensatorios de acuerdo al caso que sea necesario.
- En el caso de los APLAZAMIENTO de riegos, se deben establecer planes y cronogramas para solucionar los potenciales problemas que pueden ocasionar.

- En el caso de ACEPTACION de riesgos, documentar las características de estas vulnerabilidades para establecer un procedimiento para que cuando sea posible mediante inversión económica o nueva tecnología este pueda ser mitigado o gestionado.